cryptovision SMAERS – Java Card applet providing Security Module Application for Electronic Record-keeping Systems

Security Target Lite

BSI-DSZ-CC-1170

Common Criteria / ISO 15408

EAL 2+

Document Version 2.6 • 2023-03-21

cv cryptovision GmbH • Munscheidstr. 14 • 45886 Gelsenkirchen • Germany
www.cryptovision.com • info@cryptovision.com • +49-209-167-2450

Content

Version Control

Version	Date	Author	Changes to Previous Version
2.6	2023-03-21	Thomas Zeggel	ST Lite based on ST version 2.6.

1 Introduction

1.1 ST/TOE Identification

Title:	cryptovision SMAERS – Java Card applet providing Security Module Application for Electronic Record-keeping Systems– Security Target Lite
Document Version:	v2.6
Origin:	cv cryptovision GmbH
Compliant to:	Common Criteria Protection Profile – Security Module Application for Electronic Record-keeping Systems, BSI-CC-PP-0105-V2-2020 [PP0105]
TOE identification:	cryptovision SMAERS – Java Card applet providing Security Module Application for Electronic Record-keeping Systems, version 2.0
Short TOE name:	cryptovision SMAERS
CSP platform:	cryptovision CSP version 2.0
Javacard OS platform:	NXP JCOP 4.7 SE051, NSCIB-CC-0095534, [Zert_Javacard]
TOE documentation:	Administration and user guide [Guidance], [Guidance_OPE]

1.2 ST overview

This document contains the security target for the product cryptovision SMAERS – Java Card applet providing Security Module Application for Electronic Record-keeping Systems – for a Common Criteria certification according to EAL2. It is designed to be used exclusively on the cryptovision CSP, which is certified according to CC EAL 4+ ([PP CSP] with PP-module [PPC-CSP-TS-Au]) and itself is a composite product based on the NXP JCOP 4.7 SE051 Javacard OS platform, which is certified according to CC EAL 6+ [Zert_Javacard].

This security target defines the security objectives and requirements for the cryptovision SMAERS.

This security target claims strict conformance to the Protection Profile *Common Criteria Protection Profile – Security Module Application for Electronic Record-keeping Systems*, BSI-CC-PP-V2-0105-2020 [PP0105]. The main objectives of this ST are:

- to introduce the TOE (SMAERS application),
- to define the scope of the TOE and its security features,
- to describe the security environment of the TOE, including the assets to be protected and the threats to be countered by the TOE and its environment during the product development, production and usage,
- to describe the security objectives of the TOE and its environment supporting in terms of integrity and confidentiality of application data and programs and of protection of the TOE,
- to specify the security requirements which includes the TOE security functional requirements, the TOE assurance requirements and TOE security functionalities.

The assurance level for the TOE is CC EAL2 augmented with ALC_LCD.1 and ALC_CMS.3.

1.3 TOE overview

The TOE overview follows the description in the protection profile [PP0105].

1.3.1 Introduction

In order to combat tax-fraud, electronic record-keeping systems in Germany must be equipped with a 'Certified Technical Security System' (CTSS; 'Zertifizierte Technische Sicherheitseinrichtung') that consists of a storage medium, a security module, and a unified digital interface. The security module is subject to common criteria security certifications. W.r.t. to security requirements for the security module – defined by Bundesamt für Sicherheit in der Informationstechnik – the module consists of two components:

1. an application component that handles the business logic and functionality required to serve an electronic record-keeping system. This component is dubbed the security module application for electronic record-keeping systems (SMAERS).
2. a generic and reusable cryptographic component that implements the core cryptographic functionality required. This component is dubbed cryptographic service provider (CSP).

This security target defines the security requirements of the SMAERS component provided by cryptovision. Depending on the overall architecture, different security requirements exist for a CSP. These are defined in two protection profiles and protection profile configurations. For details on allowed architectures and required protection profiles and configurations, cf. below, in particular Section Non-TOE Hardware/ Software/ Firmware available to the TOE.

In the following, the abbreviation CSP is redundantly used for all allowed configurations mentioned.

1.3.2 TOE type

The Target of Evaluation (TOE) is a security module application implemented as software running on the CSP platform (referred to as platform architecture in [PP CSP]).

The TOE has to securely store sensitive objects (user data and TSF data, see assets). The CSP platform provides suitable mechanisms for this that may be used by the TOE.

The TOE relies on the CSP for all cryptographic operations except for the implementation for the trusted channel. In addition the TOE must rely on the platform in case of update code package verification

1.3.3 TOE definition

The TOE is a security module application as part of the security module of a certified technical security system (CTSS) for electronic record-keeping systems (ERS). Figure 1 describes the interaction between TOE and non-TOE components.

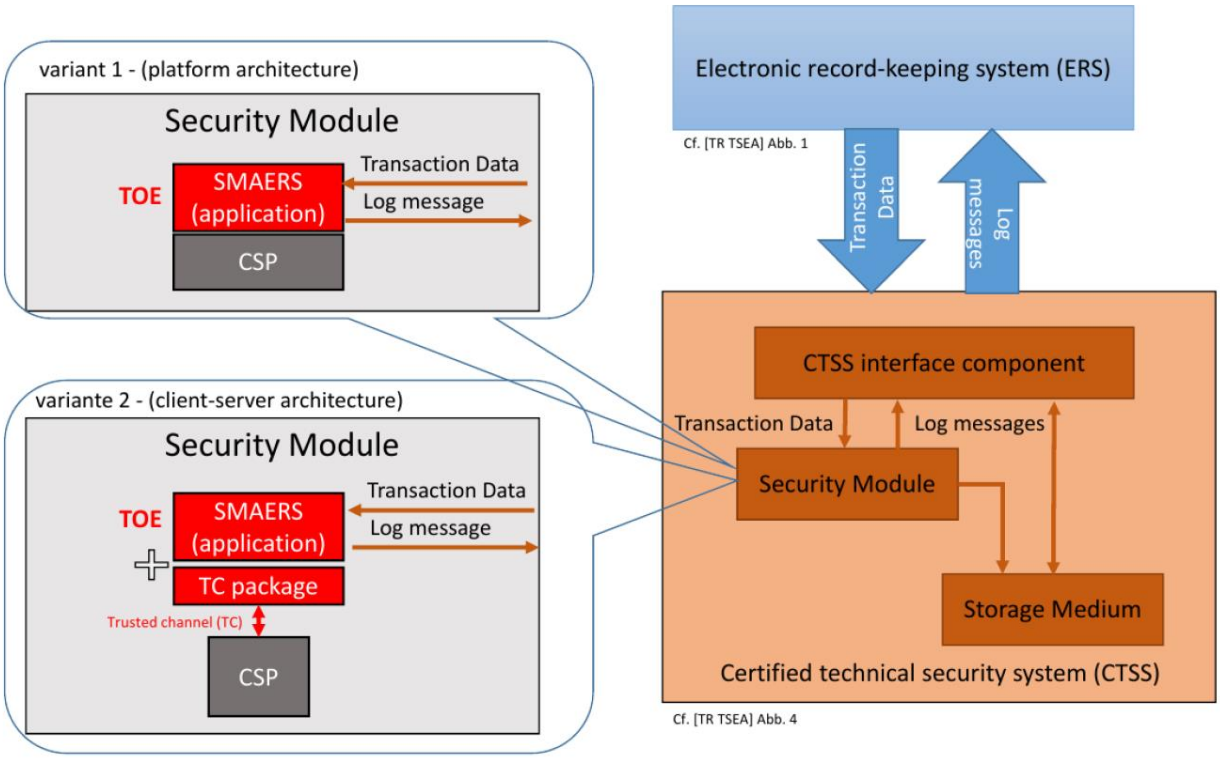

Figure 1: Description and interaction between the TOE and the relevant non-TOE components

The CTSS consists of a security module, a storage medium and an CTSS interface component providing the standardized digital interface (cf. [FCG], section 146a, paragraph 1, sentence 3) for the electronic record-keeping system and cash inspection (cf. [FCG], section 146b). The [KSV] section 2 requires the security module to provide

- the point in time when the transaction starts (cf. [KSV] section 2 sentence 2 number 1),
- the transaction number (cf. [KSV] section 2 sentence 2 number 2),
- the point in time when the transaction is completed or terminated (cf. [KSV] section 2 sentence 2 number 6), and
- the check value (cf. [KSV] section 2 sentence 2 number 7).

The security module provides the logging of transactions and other audit-relevant processes in the form of log messages (cf. [TR TSEA], Chapter 3.1). Log messages are created by the TOE using the CSP.

Log messages consist of either certified data or audit data [TR SE], as well as protocol data and a signature. There are three types of log messages, i.e. transaction logs, system logs and audit logs, cf. [TR SE] and [PP0105], Appendix: Log Message Structure and Data Dependency.

Transaction logs are created to protect the actual transaction data of the electronic record-keeping system as certified data. They are generated whenever a transaction is started, finished (i.e. completed or terminated), and may be generated when transaction data are updated. The protocol data of transaction logs contain the transaction number of the transaction and time stamps. All transaction logs with the same transaction number build together the required data of the fiscal transaction according to [KSV] Section 2, Sentence 2.

System logs are generated to log the execution of system operations as described in [TR SE] and TSF security events.

Audit logs are generated to document management or configuration operations of the CSP. The audit data of audit logs provide information for the interpretation of the transaction logs, e.g. providing information about setting or readjusting the time source that is used for time stamps.

The TOE

- imports transaction data from the CTSS interface component and includes it as certified data in a transaction log,
- generates part of the protocol data for the transaction log including
  - the transaction number generated by the TSF,
  - the serial number included by the TSF for verification of the digital signature (keyID),
- includes the timestamp, signature counter and digital signature created by the CSP over the certified data and the protocol data in the transaction log and system log,
- imports audit records from the CSP (cf. FAU_GEN.1) and exports them as audit log[1],
- generates a system log consisting of commands and TSF security events as certified data,
- exports all types of log messages to the CTSS interface component,
- provides identification and authentication of users, access control and security management of the TSF for authorized users by using cryptographic services of the CSP.

The signature counter enumerating the signatures created for log messages and the time stamps when the signature was created are generated by the CSP and are part of the protocol data.

The main part of protection profoile [PP0105] assumes the TOE being implemented as software running on a component that is physically separated from the CSP in a client-server architecture, cf. [PP CSP][PP CSPL]).

This is not the case for the TOE of this security target, thus it doesn't claim the package trusted channel between the TOE and the CSP in Chapter 7 of [PP0105].

The TOE of this security target is running on a CSP where the CSP serves as a secure execution platform, cf. platform architecture [PP CSP]. The TOE is compliant to BSI Technical Guideline TR-03153 [TR TSEA], and uses cryptographic services of the CSP compliant with BSI Technical Guideline TR-03116-5 [TR CryAS].

1.3.4 Method of use

The TOE is part of the security module of the CTSS protecting accounts and records of one or more electronic record-keeping systems. If more than one electronic record-keeping system uses the TOE the serial number of ERS (clientID) sending input must be identifiable and known to the TOE for selecting the signature-creation key.

The TOE generates time stamped and signed log messages using the CSP's cryptographic services in order to generate verifiable sequences of transaction data and log messages for cash register inspection, cf. [FCG], Section 146b.

The TOE provides security management features of the TSF for administrators. The security management features are used to configure the communication channels between the TOE with the CTSS interface component and the CSP. The TOE may support the security management functionality of the CSP by providing a communication interface to an administrator[2] or other services, e.g. to a time server.

[1] A CSP meeting BSI TR-03151 [TR SE] shall export audit records in a format suitable to directly create Audit logs, e.g. by allowing for (hashed) protocol data as additional input for the signed export of audit records.

[2] This is the case for the TOE, which comprises the interface for an „time admin" to set the internal time of the CSP.

The TOE requires the platform to support receiving and verifying the integrity of update code packages (UCPs) for installation of a new certified TOE.

1.3.5 TOE Life Cycle

The TOE life cycle is part of the life cycle of the CTSS. The life cycle documentation shall describe the complete life cycle of the CTSS including details necessary for the understanding of the interaction with and configuration of the CSP including. While only the TOE life cycle is part of the common criteria certification the additional documentation has to be provided within the certification process and has to be approved by BSI in a separate process.

The additional documentation must address, but is not limited to the following documents:

- The provisioning of the CSP within the life cycle of the CTSS describing the initial personalization and subsequent renewal of keying material used in the context of the TOE, the assignment and separation of users and roles contained in the CSP, and the audit configuration of the CSP.
- The update procedures to allow for recovery from security incidents including the procedures for creating, distributing, and enforcing installation of update code packages for the TOE and the CSP,
- The PKI concept of the underlying public key infrastructure (PKI) and the audit reports of the involved trust centers to ensure the correct identification of the taxpayer, the binding of the CTSS and keying material to the taxpayer, and the verifiability of generated signatures by third parties.

If any steps within the CTSS life cycle are delegated to an external entity, e.g. an integrator, the additional life cycle documentation must explicitly define the entities and their obligations.

Additional documentation must be provided in the following cases:

- If the client-server model is used, the personalization and management of the password used to protect the trusted channel between the TOE and the CSP must be described.
- If a CSPLight is used instead of a CSP, it must be securely operated in an environment certified according to ISO/IEC 27001. The operator must implement and continuously maintain an information security management system (ISMS) with security level high according to Appendix: Operational Requirements for CSPLight.

1.3.6 Non-TOE Hardware/Software/Firmware available to the TOE

The TOE requires

- a CSP. The CSP must be certified according to one of the following protection profiles:
  - Common Criteria Protection Profile Configuration Cryptographic Service Provider – Time Stamp Service and Audit [PPC-CSP-TS-Au]
  - Common Criteria Protection Profile Configuration Cryptographic Service Provider – Time Stamp Service, Audit and Clustering [PPC-CSP-TS-Au-Cl]
  - Common Criteria Protection Profile Configuration Cryptographic Service Provider Light – Time Stamp Service, Audit and Clustering [PPC-CSPLight-TS-Au-Cl] running on hardware that meets Appendix: Operational Requirements for CSPLight.
- a CTSS interface component that provides the transaction data and receives log messages
- an underlying platform with a secure storage (see OE.SMAERSPlatform).

The security target has to reference a fully defined API description of the CSP: cf. [AGD_PRE_CSP], [AGD_OPE_CSP].

The CSP shall meet [TR CryAS].

1.3.7 TOE and TOE platform

The specific Target of Evaluation (TOE) of this ST (Cryptovision SMAERS) is an application to be used on the Cryptovision CSP, which is certified according to [PP CSP] with PP-module [PPC-CSP-TS-Au]. The TOE is a security module application implemented as software running on the CSP platform (referred as Platform architecture in [PP0104]).

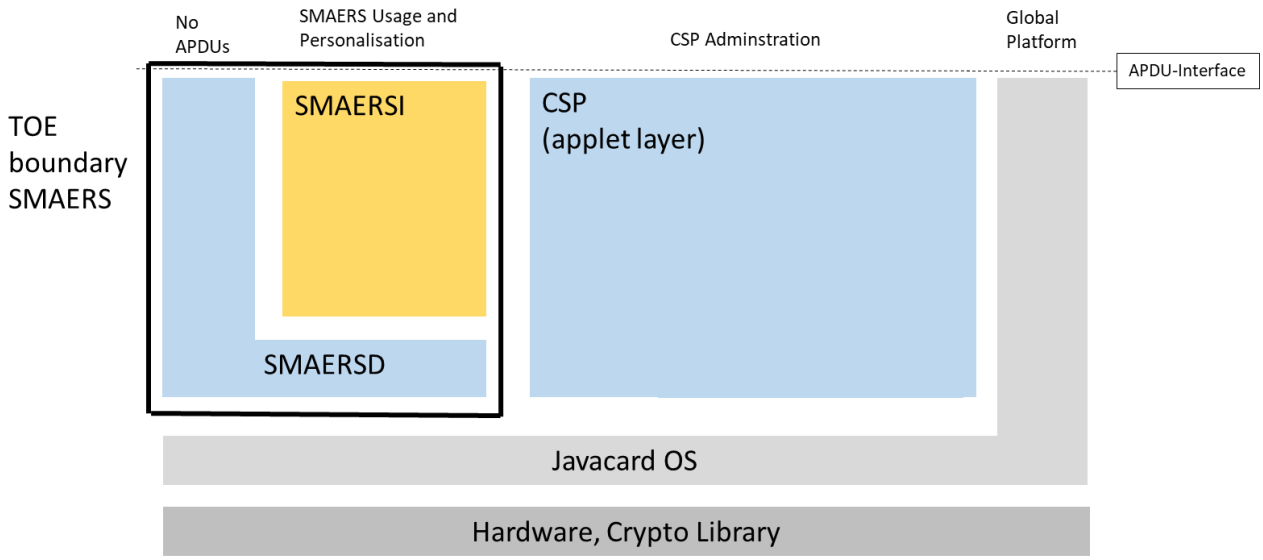

Figure 3: Structure of the TOE (SMAERS) and TOE boundary.

The SMAERS application consists of a data storage applet (SMAERSD) and a separate applet implementing the logic functionality and the APDU interface. Security functionality is provided by the CSP platform.

When updating the SMAERS application, data reside in the SMAERSD applet, while the SMAERSI applet can be updated. Thus, all internal data are unchanged by the update process.

1.3.8 Major security features of the TOE

The TOE provides the security functionality as described in section 1.3.4. The specific cryptographic functionality is completely provided by the CSP platform and described in detail in [ST_CSP].

1.3.9 TOE identification

Identification of the TOE is performed by a GET DATA command according to the procedure described in [AGD_PRE], section 3.2.4.

1.4 TOE life cycle

The TOE lifecycle is not defined in the protection profile [PP0105].

1.4.1 Development and delivery of the TOE

The target platform of the TOE (cryptovision SMAERS) is the cryptovision CSP. The cryptovision CSP comprises of the NXP JCOP 4.7 SE051 product, which itself is a composite product based on the certified hard-

ware, certified crypto library and the certified Java card operating system layer. The development and certification of the NXP JCOP 4.7 SE051 product is in the hands of NXP. The CSP package of cryptovision adds the necessary functionality to this Java Card platform to build a CSP according to [PP0104] and [PPC-CSP-TS-Au].

The cryptovision SMAERS was developed at cryptovision to add the functionality necessary to be used in a TSE technical device[3] according to the technical guidelines [TR-03151] and [TR-03153].

After completion of the development, the SMAERS application is delivered from cryptovision to NXP (for integration in a flash image) or an other third party in a secure way (encrypted and digitally signed) and stored in the secure network of cryptovision.

This delivery is the delivery of the TOE (SMAERS) according to Common Criteria.

1.4.2 Loading of the TOE

Please note that the following steps are outside of the scope of the Common Criteria certification.

The TOE (the SMAERS application) is integrated into the flash image at NXP or loaded on the CSP at a third party using standard Global platform mechanisms including delegated management. If loaded at a third party, the CSP has been produced previously based on the CSP application and encrypted keys delivered by cryptovision and JCOP4 Java Card OS chips delivered by NXP.

The loading of the SMAERS application is secured by Global platform mechanisms provided by the CSP (i.e., the JCOP4 Java card platform).

The main signature key of each SMAERS/CSP combination (embedded in the TSE) is generated on-card, the public key is exported and a certificate is generated using certified standard procedures of a certified PKI (certified according to BSI TR-03145 [TR03145]). This certificate is stored in the SMAERS application.

Afterwards, the TOE is delivered to the end-customer (embedded in the TSE)

1.5 TOE deliverables

The TOE is delivered in a PGP encrypted and signed email. The delivery constitutes the following items:

- SMAERSI applet, Version 0x0200 (Revision 0x4580), embedded in APDUs with encrypted load files and digitally signed using DAP.
- SMAERSD applet, Version 0x0200 (Revision 0x4580), embedded in APDUs with encrypted load files and digitally signed using DAP.
- Preparation Guidance (AGD_PRE) as PDF file [Guidance].
- Operational Guidance (AGD_OPE) as PDF file [Guidance-OPE].

Besides delivery, the TOE is also stored at cryptovision.

[3] Technische Sicherheitseinrichtung

2 Conformance claims

2.1 CC conformance claims

The security target claims conformance to CC version 3.1 revision 5.

Conformance of this security target with respect to CC Part 2 [CC_2] (security functional components) is CC Part 2.

Conformance of this security target with respect to CC Part 3 [CC_3] (security assurance components) is CC Part 3 conformant.

2.2 Package claim

This security target claims conformance to EAL2 augmented with ALC_LCD.1 and ALC_CMS.3.

2.3 PP claim

This security target claims **strict conformance** to

- Common Criteria Protection Profile – Security Module Application for Electronic Record-keeping Systems, BSI-CC-PP-0105-2020-V2 [PP0105].

2.4 Conformance rationale

The dependencies of security assurance components of the package EAL2 are solved within the package [CC_3]. The components ALC_LCD.1 and ALC_CMS.3 have no dependencies on other components.

2.5 Dedicated platform

The TOE is dedicated to be used on the platform cryptovision CSP, which is certified according to [PP CSP] with PP-module [PPC-CSP-TS-Au].

The identification of the platform is described in [Guidance], section 3.2.4.

3 Security problem definition

This chapter has been taken from [PP0105].

3.1 Introduction

3.1.1 Assets

The assets of the TOE are

- the transaction data provided by the CTSS interface component, where authenticity and integrity including completeness of the transaction data shall be protected, i.e. verification of the transaction log messages shall determine whether the transaction data was received from the CTSS interface component, and modifications and gaps shall be detectable,
- the transaction number (as part of the transaction data) that enumerates transactions. The transaction number must be continuously increasing without gaps.
- the audit records imported from the CSP and exported as audit logs to the CTSS interface component, the system logs and transaction logs
- the update code package (UCP) and the UCP version number
- the PACE password to setup the trusted channel to the CSP (only in case the package 'Trusted Channel' is claimed).

The CSP protects and enumerates its audit records against undetected modification and gaps.

Asset	Protection
transaction data	authenticity, integrity
transaction number	authenticity, integrity
audit logs/audit records, system logs and transaction logs	authenticity, integrity
update code package	authenticity
UCP version number	integrity

Table 1: Assets to be protected by the TOE

3.1.2 Users and subjects

The users and subjects defined below are distinct from the role model in [TR SE]. Users and roles defined in the latter, including e.g. the taxpayer acting as (CTSS-)administrator, converge in the CTSS interface component.

The TOE knows users as external entities active communicating with the TOE as

- electronic record-keeping system (ERS),
- CTSS interface component,
- CSP,
- (SMAERS-) administrator.

The ERS is tested by the TOE as an external entity and communicates with the TOE through the CTSS interface component. The TOE also uses the CTSS interface component as a passive external entity for the storage of transaction logs, system logs, and audit logs. The TOE uses the CSP as external entity providing security services and audit records.

The (SMAERS-) administrator is assumed to be the TOE manufacturer or an integrator acting on behalf of the manufacturer and must not be the taxpayer.

The subjects as active entities in the TOE perform operations on objects and obtain their associated security attributes from the authenticated users on whose behalf they are acting, or by default.

3.1.3 Roles

The TOE knows at least the following roles taken by a user or a subject acting on behalf of a user:

- role unidentified user: This role is associated with any user not (successfully) identified by the TOE. This role is assumed for subjects after start-up of the TOE and deactivated CTSS interface component. The TOE allows users in this role to run self-test of the TOE.
- role administrator: A user in this role is allowed to perform management functions. The administrator subject is acting on behalf of a human user after successful authentication as administrator until logout.
- role CTSS interface: A subject in this role is allowed to import Transaction Data from CTSS interface component, to generate transaction logs and system logs, and to export transaction logs and system logs to the CTSS interface component. A subject in this role is started automatically after start-up of the TOE if the CTSS interface role is activated and the CTSS interface component and the CSP are successfully tested according to FPT_TEE.1. The ERS uses the CTSS role.
- CSP role: A subject in this role is allowed to import audit records from CSP and to export Audit logs to the CTSS interface component. In addition the CSP role is allowed to start the update process. A subject in CSP role is started automatically after start-up of the TOE if the CSP is successfully tested according to FPT_TEE.1.
- role CTSS administrator: The CTSS administrator is allowed to lock and unlock transaction logging, trigger the update functionality and to terminate the TOE after successful authentication. This role was added to the roles of the SMAERS protection profile []PP0105 because of the definition in TR-03153 [TR TSEA].
- role time administrator: A role that is allowed to set the time of the TOE in operational state.

3.1.4 Objects

The TSF operates on the following types of user data objects

- transaction data (TD),
- audit records,
- data-to-be-signed (DTBS),
- protocolData with signature containing the time stamp, the signature counter, and the digital signature; all generated by the CSP (cf. [TR SE] and [TR TSEA]),
- log messages (LM) as transaction log, system log or audit log,
- update code package (UCP)
- commands (type of operation).

The formats of transaction data and log messages meet [TR SE].

The CTSS interface component provides transaction data as data to be certified by means of transaction logs (cf. below).

Audit records are data imported from the CSP.

The data-to-be-signed compiled by the TSF and sent to the CSP for signing and time stamping consists of

- certified data i.e.
  - in case of a transaction log: the transaction data with the type of the certified data transaction log, object identifier (id-SE-API-transaction-log): bsi-de (0.4.0.127.0.7) applications (3) sE-API (7) sE-API-dataformats(1) 1 (cf. [TR SE], chapter 2.3.1)
  - in case of a system log: the security related events with the type of the certified data system log, object identifier (id-SE-API-system-log): bsi-de (0.4.0.127.0.7) applications (3) sE-API (7) sE-APIdataformats(1) 2 (cf. [TR SE], chapter 2.3.2)
  - in case of an audit log: the audit record with the type of the certified data audit log, object identifier (idSE-API-audit-log): bsi-de (0.4.0.127.0.7) applications (3) sE-API (7) sE-API-dataformats(1) 3 (cf. [TR SE], chapter 2.3.3)
- protocol data generated by the TSF
  - the transaction number,
  - the keyID as a hash value of the signature-verification key,
  - the type of the operation as name of the API function whose execution is recorded by the log message, i.e. StartTransaction, UpdateTransaction or FinishTransaction,
  - the optional protocol data (may be empty).

The CSP adds to the data-to-be-signed

- the point in time when the log message was created,
- the signature counter that enumerates the signatures created with the signature-creation key.

Refer to [TR SE] for details of the log messages format.

The Update Code Package (UCP) is a complete software package that is managed by the secure platform and its operating system that executes the SMAERS application. The operating system of the secure platform performs an update of the SMAERS application, it is required that the verification of the UCP is performed by the operating system prior to installation. Depending on the update procedure of the operating system either the new TOE alone or the old TOE and the new TOE together perform an upgrade by exporting and importing TSF data into the new TOE.

3.1.5 Security attributes

Users known to the TOE have the security attributes stored in an authentication data record (ADR):

- user identity (User-ID),
- authentication reference data,
- role with detailed access rights gained after successful authentication.

The CTSS interface component and CSP known to the TOE have at least the security attributes identity, cf. FIA_ATD.1.

Passwords as authentication reference data have the security attributes

- status: the values initial password and operational password,
- number of unsuccessful authentication attempts.

The transaction data (TD) have the security attributes

- clientID to determine the signature-creation key to be used for signing the Transaction log and the keyID to be included in the protocol data of the Transaction log,

- type of the operation to determine the actual transaction as StartTransaction, UpdateTransaction or FinishTransaction.
- transaction number to assign the TD to an ongoing transaction and enumerating the transactions continuously increasing without gaps.

The TOE accepts transaction data only if the clientID is known and mapped to a signature key in the CSP (keyID).

The TOE manages for each known keyID the last assigned transaction number and the transaction numbers of the ongoing transactions. If the type of the operation of imported transaction data is StartTransaction, then a new transaction is started and the TOE generates a new transaction number by addition of 1 to the last assigned transaction number, includes this value in the protocol data of the transaction log returned to the CTSS interface component, and add this value to the list of ongoing transaction. If the type of the operation is UpdateTransaction or FinishTransaction and meets the transaction number of an ongoing transaction, the transaction number in the transaction data is imported and assigned to the protocol data of the transaction log. If the type of the operation is FinishTransaction or the transaction is terminated by the TOE, the transaction number is removed from the list of ongoing transactions cf. [TR SE].

A UCP has the security attributes

- issuer: identifier of the authorized issuer of the UCP signing the UCP,
- signature: digital signature of the UCP generated by the authorized issuer,
- version number.

3.1.6 Log messages

Log messages include at least the following security attributes and the signature used by the tax inspector of the cash register inspection

- signature counter enumerating the log message continuously increasing without gaps,
- time stamp as time when the log message was created,
- keyID to determine the certificate to be used for the verification of the digital signatures as a check value of the transaction data.

The following security attributes are conditional in log messages:

- Transaction logs contain the security attribute transaction number assigning the log message to the transaction of the electronic record-keeping system and the type of operation, i.e start, update or finish transaction.
- System logs contain the security attribute event assigning the log message to the security related event of the TSF.
- Audit logs contain the security attribute audit record assigning the log message to security related events of the CSP.

3.2 Threats

3.2.1 T.EvadTD Evading Transaction Data

The attacker prevents sending to the TOE legally required transaction data in order to avoid generation of valid Transaction logs..

3.2.2 T.ManipTD Manipulation of Transaction Data

The attacker manipulates transaction data sent by the electronic record-keeping system through the CTSS interface component to the TOE, or generates forged transaction data and sends them to the TOE in order to generate incorrect transaction logs.

3.2.3 T.ManipDTBS Manipulation of Data-To Be-Signed-And-Time-Stamped

The attacker generates forged or manipulates Data-To-Be-Signed sent for signing and time stamping to the CSP. A forged transaction log may result in forged transaction data provided for cash inspection. A forged audit log or system log may result in faulty interpretation of the transaction data.

3.2.4 T.ManipLM Manipulation of a Log Message

The attacker manipulates without detection a log message exported to the CTSS interface component. This log message is then used for cash inspection.

3.2.5 T.ManipLMS Manipulation of a Log Message Sequence

The attacker manipulates without detection the log message sequence exported to the CTSS interface component. This log message sequence is then used for cash inspection.

3.2.6 T.ManipTN Manipulation of Transaction Number

The attacker manipulates the TOE internal transaction number used in log messages.

3.2.7 T.FaUpD Faulty Update Code Package

An attacker deploys an unauthorized manipulated update code package or restores a previous TSF implementation enabling attacks against integrity of TSF implementation, or confidentiality and integrity of user data or TSF data after installation of the manipulated update code package.

Application note 1: The taxpayer is the subject that owns and operates the ERS and CTSS (either directly or indirectly). The taxpayer is assumed to use an ERS equipped with a CTSS, to prevent misuse of the ERS by unauthorized persons, and to correctly tally all transactions with the ERS as required by law (c.f. OSP.SecERS and OSP.ProtDev). The TOE does not protect against threats that result from temporarily or permanently not using an ERS as required by law. The taxpayer is however also considered as potential attacker, who may use a manipulated CTSS or manipulates logs after they were produced by the CTSS.

3.3 Organisational security policies

3.3.1 OSP.SecERS Secure use of the Electronic Record-Keeping System

The taxpayer shall use an electronic record-keeping system to generate accounts, records and receipts. The electronic record-keeping system shall record separately, correctly, completely, and in real time accounts and records on all transactions that are legally required (cf. [FCG] section 146a (1) sentence 1). The receipt shall include besides the transaction data the points in time when the transaction is started, completed or terminated, and the transaction number provided by the certified security device (cf. [KSV] section 6 sentence 1).

3.3.2 OSP.CertSecDev Certified Security Device

The electronic record-keeping system and the accounts and records generated by the electronic record-keeping system shall be protected by a certified security device; cf. [FCG], Section 146a (1), Sentence 2. The security module of the certified security device generates time stamps of the start, completion, and termination of a transaction, as well as a transaction number; cf. [KSV], Section 2, Sentence 3.

3.3.3 OSP.ProtDev Protection of Electronic Record-Keeping System and Certified Security Service

The taxpayer shall correctly operate the electronic record-keeping system (cf. [FCG], Section 379 (1), Sentence 1, Number 4), and correctly protect the electronic record-keeping system and the certified security device; cf. [FCG], Section 379 (1), Sentence 1, Numbers 5.

3.3.4 OSP.ValidTrans Validation of transactions

A sequence of transactions is valid if (1) all Log messages meet the requirements for content defined in [KSV] section 2, (2) their check values according to [KSV] section 2 sentence 2 number 7 are valid digital signatures, (3) the transaction numbers are consecutive increasing without gaps (cf. [KSV] section 2 sentence 4), and (4) the points in time when the transaction starts are monotonic increasing. The sequence of Log messages support detection of incomplete transactions and manipulations.

3.3.5 OSP.Update Authorized Update Code Packages

Update Code Packages are delivered to the TOE from the platform and are signed by the authorized issuer. The platform verifies the authenticity of the received Update Code Package before installation.

Application note 2: The update is performed by the platform provided by the operational environment, c.f. OE.CSPPlatform for the platform architecture or OE.SMAERSPlatform for the client-server architecture.

3.4 Assumptions

3.4.1 A.SMAERSPlatform Secure platform storage

The platform that executes the TOE provide mechanisms to preserve the confidentiality, integrity and to prevent rollback of stored sensitive objects, including the TOE software itself.

3.4.2 A.CSP Cryptographic service provider

A CSP is either remotely accessible via trusted channel to the TOE (client-server architecture) and certified as compliant to [PPC-CSP-TS-Au], [PPC-CSP-TS-Au-Cl], or [PPC-CSPLight-TS-Au-Cl] running on hardware that meets Appendix: Operational Requirements for CSPLight as well as the requirements in chapter 1.2 section “TOE Life Cycle”

Or, the operational environment provides a cryptographic service provider for the TOE that is certified as compliant to [PPC-CSP-TS-Au] or [PPC-CSP-TS-Au-Cl] (platform architecture).

The CSP exports audit records in form of audit logs meeting [TR SE]. Also, the CSP must provide a fully defined API description.

3.4.3 A.ProtComCSP Protection of Communication between TOE and CSP

The integrity of the communication data between TOE and CSP in the client-server architecture is protected via a trusted channel, and the security target must claim the package Trusted Channel, defined in Chapter 7. In case of the platform architecture of the CSP, the CSP provides a secure execution environment for the TOE and protects the integrity of communication data with the TOE directly using the security services of the CSP.

3.4.4 A.ProtComERS Protection of Communication between TOE and Electronic Record-Keeping System

The electronic record-keeping system provides transaction data whenever a transaction starts, transaction data are updated, or when the transaction is completed or terminated. The ERS and the TOE must be contained in the same physical operational environment that must protect the integrity of communication data between the TOE and the electronic record-keeping system, see Figure 2.

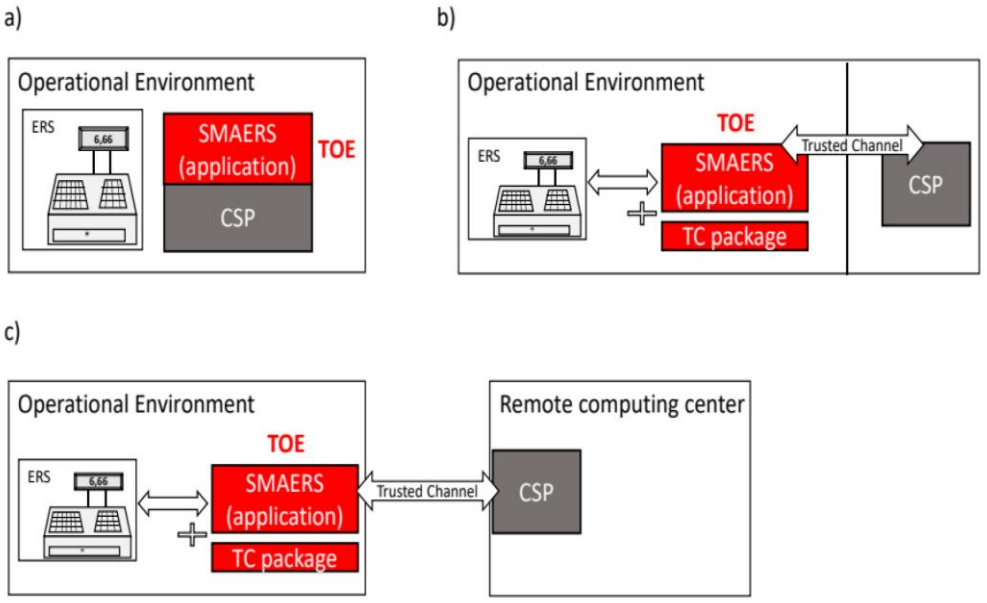

Figure 2: The TOE is always operated as a local component. a) platform architecture b) client-server architecture with local computing center c) client-server architecture with remote computing center. The TOE of the ST uses (a).

3.4.5 A.VerifLMS Verification of Log Message Sequences

The operational environment verifies the digital signatures, the transaction numbers and the time stamps of log messages in sequence in order to detect forged or missing log messages. The certificate of the signature verification data is securely distributed to the tax inspector. The tax inspector ensures that the transactions are created by a certified security module, e.g. in form of test transactions.

3.4.6 A.Admin Trustworthy Administrator

The administrator acts in a trustworthy way and must be independent of the taxpayer (cf. PP Application note 1).

4 Security Objectives

This chapter describes the security objectives for the TOE and the security objectives for the TOE environment. The content has been taken from [PP0105].

4.1 Security Objectives for the TOE

This section describes the security objectives for the TOE addressing the aspects of identified threats to be countered by the TOE and organizational security policies to be met by the TOE.

4.1.1 O.GenLM Generation of Log Messages

The TSF shall generate transaction logs containing

- transaction data, transaction number created by the TSF, and
- time stamps and digital signatures created by the cryptographic service provider.

The TSF shall generate system logs.

4.1.2 O.ImpExp Import of Transaction Data from and Export of Log Messages to CTSS Interface Component

The TSF shall import transaction data from the electronic record-keeping system through the CTSS interface component, import audit records from the CSP and export log messages to the CTSS interface component.

4.1.3 O.IAA Authentication of Administrators

The TOE shall verify the claimed identity of the administrators by means of password.

4.1.4 O.SecMan Security Management

The TOE shall restrict the security management of TSF and TSF data to authenticated administrators. The TSF prevents management of the transaction number generation.

4.1.5 O.TEE Test of External Entities

The TSF shall test the presence and identity of the electronic record-keeping system and cryptographic service provider connected to the TOE, and allow generation of transaction logs only if both pass the tests, and must enter a secure state if any test fails.

4.1.6 O.TST Self-Test and Secure State

The TSF shall perform self-tests. The TSF enters a secure state if the self-test fails, or the test of the presence and identity of the electronic record-keeping system fails, or the test of the presence and identity of cryptographic service provider fails. It shall also test for new succesfully installed update code packages and the correctness of the increased version number.

4.1.7 O.ImpExpUCP Secure Import and Export of User Data

The TSF shall securely export the user data and TSF data to the secure storage of the platform and import the user data and TSF data after the successful update process.

4.2 Security Objectives for the Operational Environment

4.2.1 OE.ERS Trustworthy Electronic Record-Keeping System

The taxpayer shall correctly use an electronic record-keeping system that provides separately, correctly, completely and in real time all transaction data that are legally required for the generation of log messages to the TOE (cf. PP Application Note 1). The electronic record-keeping system shall support testing its presence and identity as an external entity by the TOE. The electronic record-keeping system shall produce receipts including not only the transaction data, but also the points in time whenever a transaction is started, completed or terminated, as well as the transaction number provided by the certified security device.

4.2.2 OE.SMAERS Platform Secure platform storage

The platform that executes the TOE has to ensure the integrity of the TOE itself and to provide secure storage which protects the integrity and confidentiality of stored security relevant objects as required (cf. Chapter 1.2 “TOE Type”). The platform verifies and installs the UCP.

4.2.3 OE.CSP Cryptographic Service Provider Component

A CSP must be either remotely accessible via a trusted channel to the TOE (client-server architecture) and certified as compliant to [PPC-CSP-TS-Au], [PPC-CSP-TS-Au-Cl], or [PPC-CSPLight-TS-Au-Cl] running on hardware that meets Appendix: Operational Requirements for CSPLight.

Or, the operational environment shall provide a cryptographic service provider for the TOE that is certified as compliant to [PPC-CSP-TS-Au] or [PPC-CSP-TS-Au-Cl], i.e. using the platform architecture.

The CSP shall export audit records in form of audit logs meeting [TR SE].

PP application note 3: The Common Criteria Protection Profile Configurations [PPC-CSP-TS-Au], [PPC-CSP-TSAu-Cl], and [PPC-CSPLight-TS-Au-Cl] require the cryptographic service provider to provide security services to digitally sign transaction data, to verify a signature of an update code package, and for time services. The CSP audit records shall be exported meeting [TR SE] in order to avoid a transformation of an audit record into a log message. The vendor of the TOE may provide the TOE together with a certified cryptographic service provider.[4]

4.2.4 OE.CSPPlatform CSP as Secure Platform of the TOE

In case of the platform architecture[5] the CSP provides a secure execution environment and security services for the TOE running on top.

PP application note 3: <applied>

4.2.5 OE.Transaction Verification of Transaction

The operational environment shall verify the validity of log message sequences by verification of the corresponding digital signatures, shall verify the transaction numbers as being consecutive without gaps, and shall verify the points in time when the transaction starts as being consecutively

[4] The TOE of this ST is provided together with a cryptographic service provider (cryptovision CSP).

[5] This is the case for the TOE.

increasing with increasing transaction numbers, and consider the log messages. The taxpayer shall ensure that the cryptographic service provider holds digital signature creation data and a corresponding valid certificate. The certificate shall be securely distributed to the tax inspector.

4.2.6 OE.SecOEnv Secure Operational Environment

The operational environment shall protect the integrity of the communication between the electronic record-keeping system and the TOE. The administrator shall act in a trustworthy way and is assumed to be the manufacturer or integrator. The administrator must be independent of the taxpayer.

4.2.7 OE.SecCommCSP Secure communication between TOE and CSP

The security target shall claim the package trusted channel (Chapter 7) to protect the integrity of the communication between the TOE and the CSP in the client-server architecture. In case of the platform architecture, the operational environment shall protect the integrity of the communication between the TOE and the cryptographic service provider.

4.2.8 OE.SUCP Signed Update Code Packages

The manufacturer shall issue digitally signed update code packages together with its security attributes.

4.2.9 OE.SecUCP Secure download and authorized use of Update Code Package

The platform shall verify the authenticity of received update code packages and install only authentic update code packages.

4.3 Security Objective Rationale

The following table traces a security objective for the TOE back to threats countered by that security objective and OSPs enforced by that security objective, and a security objective for the operational environment back to threats countered by that security objective, OSPs enforced by that security objective, and assumptions upheld by that security objective.

The rationale has been taken from the protection profile [PP0105].

	T.EvadTD	T.ManipTD	T.ManipDTBS	T.ManipLM	T.ManipLMS	T.ManipTN	T.FaUpD	OSP.SecERS	OSP.CertSecDev	OSP.ProtDev	OSP.ValidTrans	OSP.Update	A.CSP	A.SMAERSPlatform	A.ProtComCSP	A.ProtComERS	A.VerifLMS	A.Admin
O.GenLM	x			x	x						x							
O.IAA				x							x							
O.ImpExp					x						x							

	T.EvadTD	T.ManipTD	T.ManipDTBS	T.ManipLM	T.ManipLMS	T.ManipTN	T.FaUpD	OSP.SecERS	OSP.CertSecDev	OSP.ProtDev	OSP.ValidTrans	OSP.Update	A.CSP	A.SMAERSPlatform	A.ProtComCSP	A.ProtComERS	A.VerifLMS	A.Admin
O.SecMan						x					x							
O.TEE	x	x	x	x	x			x										
O.TST				x			x											
O.ImpExpUCP							x					x						
OE.CSP				x					x				x					
OE.SMAERSPlatform		x	x				x							x				
OE.CSPPlatform			x												x			
OE.ERS	x	x						x										
OE.SecUCP							x					x						
OE.SecCommCSP			x												x			
OE.SecOEnv	x			x	x			x		x						x		x
OE.SUCP							x					x						
OE.Transaction											x						x	

Table 2: Security Objective Rationale

The following part of the chapter demonstrates that the security objectives counter all threats and enforce all OSPs, and the security objectives for the operational environment uphold all assumptions.

The threat T.EvadTD Evading Transaction Data is mitigated by:

- The security objective for the TOE O.GenLM requiring the TSF to create transaction logs containing transaction data and a transaction number generated by the TSF, and time stamps and digital signatures, therefore allowing to decide whether presented transaction data have a corresponding transaction data set in the transaction data set sequence.
- The security objective for the TOE O.TEE requiring the TSF to test the presence and identity of the electronic record-keeping system connected to the TOE.
- The security objective for the operational environment OE.ERS requiring the taxpayer to use an electronic record-keeping system that provides completely and in real time all transaction data that are legally required for generation of log messages to the TOE.
- The security objective for the operational environment OE.SecOEnv requiring the operational environment to protect the communication between ERS and TOE against manipulation and perturbation.

The threat T.ManipTD Manipulation of Transaction Data is mitigated by:

- The security objective for the TOE O.TEE requiring the TSF to test the presence and identity of the CTSS interface component connected to the TOE,

- The security objective for the operational environment OE.ERS requiring the taxpayer to use an electronic record-keeping system that provides correctly, completely and in real time all transaction data that are legally required for generation of log messages to the TOE,
- The security objective for the operational environment OE.SMAERSPlatform requiring the operational environment to protect the TOE against manipulation and misuse.

The threat T.ManipDTBS Manipulation of Data-To-Be-Signed-And-Time-Stamped is mitigated by:

- The security objective for the TOE O.TEE requiring the TSF to test the presence and identity of the CSP connected to the TOE.
- In case of the platform architecture, the OE.CSPPlatform “CSP as Secure Platform of the TOE“ requires the CSP to provide a secure execution environment. In case of the client-server architecture, the OE.SMAERSPlatform.
- The security objective for the operational environment OE.SecCommCSP “Secure communication between TOE and CSP” ensures the protection of the integrity of the communication between the TOE and the cryptographic service provider. The operational environment shall protect the integrity of the communication between the TOE and the cryptographic service provider. In case of the client-server architecture, the TOE and the CSP component are physically separated components. The integrity of the communication between the TOE and the CSP shall be protected by means of a trusted channel as provided by the CSP according to [PPC-CSP-TS-Au][PPC-CSP-TS-Au-CL][PPC-CSPLight-TS-Au-Cl] and by the TOE claiming the package trusted channel between the TOE and the CSP, cf. Chapter 7.

The threat T.ManipLM Manipulation of Log messages is countered by:

- The security objective for the TOE O.GenLM “Generation of Log messages“ by means of digital signatures generated by the CSP, which allows to detect manipulation of transaction data sets according to OE.Transaction.
- The security objective for the TOE O.IAA requiring the TSF to authenticate administrators by means of a password.
- The security objective for the TOE O.TEE “Test of External Entities” requiring the TSF to test the presence and identity of the CSP connected to the TOE.
- The security objective for the TOE O.TST “Self-Test and Secure State” detects failure and prevents generation of transaction data sets if time source is not available or the test of the CSP fails.
- The security objectives for the operational environment OE.CSP “Cryptographic Service Provider Component” ensures the availability of a certified CSP for generation of time stamps and digital signatures, and the distribution of the certificate linked to the taxpayer for signature verification.
- The security objective for the operational environment OE.SecOEnv “Secure Operational Environment” protecting the communication between ERS and TOE.

The threat T.ManipLMS Manipulation of a Log Message Sequence is countered by:

- The security objective for the TOE O.GenLM “Generation of Log Messages” requiring the TSF to generate log messages containing transaction data imported from the electronic record-keeping system, requiring the TSF to generate time stamps whenever a transaction starts, is completed or aborted, and requiring the TSF to create a transaction number and a digital signature of the transaction data using the digital signature-creation service of the cryptographic service provider.

- The security objective for the TOE O.ImpExp “Import of Transaction Data from and Export of Log Message to CTSS Interface Component“ requiring the TSF to import transaction data from the electronic record-keeping system through the CTSS interface component and to export log messages to the CTSS interface component.
- The security objective for the TOE O.TEE “Test of External Entities” requiring the TSF to test the availability of the CTSS interface component and CSP connected to the TOE.
- The security objective for the operational environment OE.SecOEnv “Secure Operational Environment” protecting the communication between ERS and TOE.

The threat T.ManipTN Manipulation of Transaction Number is countered by the security objectives for the TOE O.SecMan TSF preventing management of transaction number generation.

The threat T.FaUpD Faulty Update Code Package is countered by:

- The security objectives for the TOE O.ImpExpUCP “Secure Import and Export of User Data” ensuring that user data are exported and imported after successful update process.
- The security objective for the TOE O.TST “Self-Test and Secure State” ensuring a correctly increased version number after installation of an update code package.
- The security objective for the operational environment OE.SUCP ensures that the authentic update code packages are signed and distributed with security attributes.
- The OE.SecUCP “Secure download and authorized use of Update Code Package” ensures that only authentic UCPs are installed.
- The OE.SMAERSPlatform ensures verifying the UCP.

The organizational security policy OSP.SecERS Secure use of the electronic record-keeping system is directly enforced by:

- The security objective for the TOE O.TEE requiring the TSF to test the presence and identity of the ERS as an external entity.
- The security objective for the operational environment OE.ERS “Trustworthy Electronic Record-Keeping System”.
- The security objective for the operational environment OE.SecOEnv “Secure Operational Environment” protecting the communication of ERS and TOE.

The organizational security policy OSP.CertSecDev Certified Security Device is directly enforced by the security objectives for the operational environment OE.CSP “Cryptographic Service Provider Component” and the certification conformant to this protection profile.

The organizational security policy OSP.ProtDev Protection of ERS and Security Module is directly ensured by the security objective for the operational environment OE.SecOEnv “Secure Operational Environment”.

The organizational security policy OSP.ValidTrans Validation of transactions is enforced by the security objectives for the TOE

- the security objective for the TOE O.GenLM “Generation of Log messages” requiring the TSF to generate log messages containing transaction data imported from the electronic record-keeping system, to generate time stamps whenever a transaction starts, is completed or aborted, and to generate a transaction number and a digital signature of the transaction data created using the digital signaturecreation service of the cryptographic service provider,
- the security objectives for the TOE O.IAA “Authentication of Administrators” requiring the TSF to authenticate administrators by means of a password,

the security objective for the TOE O.ImpExp “Import of Transaction Data from and Export of Log Message to CTSS Interface Component” requiring the TSF to import transaction data from the electronic record-keeping system through the CTSS interface component and to export log messages to the CTSS interface component.

- the security objective for the TOE O.SecMan “Security Management” preventing manipulation of the transaction numbers and limiting the authorized manipulation of the time source to administrators.
- The security objective for the operational environment OE.Transaction “Verification of Transaction” ensures the condition for verification of the digital signature of the transaction data set.

The organizational security policy OSP.Update Authorized Update Code Packages is implemented by the security objective for the operational environment OE.SUCP “Signed Update Code Packages” ensuring a digital signature of a secure update code package together with its security attributes and the security objectives for the operational environment OE.SecUCP “Secure Download and Authorized Use of Update Code Package” ensuring the verification of the digital signature.

The assumption A.CSP Cryptographic service provider is directly implemented by the security objective for the operational environment OE.CSP ”Cryptographic service provider component”.

The assumption A.SMAERSPlatform is directly implemented by the security objective for the operational environment OE.SMAERSPlatform that requires secure storage of sensitive objects.

The assumption A.ProtComCSP Protection of Communication between TOE and CSP is directly implemented by the security objectives for the operational environment OE.SecCommCSP which requires the protection of the communication between the TOE and the CSP. In case of the platform architecture, the OE.CSPPlatform requires the CSP to provide a secure execution environment. In case of the client-server architecture[6], the TOE and the CSP component are physically separated components. The integrity of the communication between the TOE and the CSP shall then be protected by means of a trusted channel as provided by the CSP according to [PPC-CSP-TS-Au], [PPC-CSP-TS-Au-Cl], or [PPC-CSPLight-TS-Au-Cl] and by the TOE claiming the package trusted channel, cf. Chapter 7.

The assumption A.ProtComERS Protection of Communication between TOE and Electronic Record-Keeping System is directly implemented by the security objective for the operational environment OE.SecOEnv “Secure Operational Environment” protecting the integrity of the communication between the electronic record-keeping system and the TOE.

The assumption A.VerifLMS Verification of Log Message Sequences is directly implemented by the security objective for the operational environment OE.Transaction “Verification of Log message Sequences”.

The assumption A.Admin Trustworthy Administrator is directly implemented by the security objective for the operational environment OE.SecOEnv “Secure Operational Environment”.

[6] Not relevant for the TOE, since it uses a secure platform architecture.

5 Extended Component Definition

The extended components defined in [PP0105] (FIA_API.1 and FCS_RNG.1) are used only in the package Package Trusted Channel between TOE and CSP, cf. chapter 7 of [PP0105], and thus are not relevant for this security target. No extended components are defined for this security target.

6 IT Security Requirements

The CC allows several operations to be performed on functional requirements; refinement, selection, assignment, and iteration are defined in paragraph 8.1 of Part 1 [CC_1] of the CC. Each of these operations is used in this ST and the underlying PP.

Operations already performed in the underlying Protection Profile [PP0105] are uniformly marked by ***bold italic*** font style; for further information on details of the operation, please refer to the protection profile.

Operations performed within this Security Target are marked by **bold underlined** font style; further information on details of the operation is provided in foot notes.

6.1 Security functional requirements

6.1.1 Security Management

6.1.1.1 FMT_SMR.1 Security roles

Hierarchical to:	No other components.
Dependencies:	FIA_UID.1 Timing of identification
FMT_SMR.1.1	The TSF shall maintain the roles: ***unidentified User, administrator, CTSS interface role and CSP role,*** **Time Administrator, CTSS Administrator**[7]***.***
FMT_SMR.1.2	The TSF shall be able to associate users with roles.

Developer note: The Time Administrator is directly connected to the according role in the CSP platform.

6.1.1.2 FMT_SMF.1 Specification of Management Functions

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FMT_SMF.1.1	The TSF shall be capable of performing the following management functions: ***(1) management of security functions behaviour (cf. FMT_MOF.1),*** ***(2) management of authentication reference data (cf. FMT_MTD.1/AD, FMT_MTD.3/PW),*** ***(3) management of security attributes (cf. FMT_MTD.3/PW, FMT_MSA.3, FMT_MSA.4),*** ***(4)*** **None**[8]***.***

Developer note: Please note that the necessary security functionality for the SFR above is provided by the CSP platform.

6.1.1.3 FMT_MOF.1 Management of security functions behaviour

Hierarchical to:	No other components.
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
FMT_MOF.1.1	The TSF shall restrict the ability to

[7] [assignment: other roles]

[8] [assignment: list additional of security management functions to be provided by the TSF]

(1) enable and disable the function ***password authentication according to FIA_UAU.5.2, clause (2) if defined*** to ***administrator,***

(2) determine the behaviour of and modify the behaviour of the function FDP_ACF.1/LM by definition of a life time limit of ongoing transactions after which the transaction is terminated by the TSF to administrator,

(3) determine the behaviour of the function FPT_TEE.1 by definition of the identity and features to be tested of ERS to administrator,

(4) determine the behaviour of the function FPT_TEE.1 by definition of the identity and features to be tested of CSP to administrator,

(5) determine the behaviour of and modify the behaviour of the function FPT_TEE.1 in case the test of CTSS interface component or CSP fails to administrator,

(6) determine the behaviour of and modify the behaviour of the functions select the auditable events according to FAU_GEN.1/SYS to administrator,

(7) determine the behaviour of and modify the behaviour of the functions automatic export of audit trails according to FAU_STG.3.1/SYS clause (1) to administrator.

PP application note 5: The refinements of FMT_MOF.1, bullet (2) to (7) are made in order to avoid iterations of the component. The life time of a transaction starts with receiving the Transaction Data with Type of Operation StartTransaction.

6.1.1.4 FMT_MSA.1 Management of security attributes

Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]
	FMT_SMR.1 Security roles
	FMT_SMF.1 Specification of Management Functions
FMT_MSA.1.1	The TSF shall enforce the ***log message SFP and update SFP*** to restrict the ability to
	(1) define the set of accepted values of the security attributes "clientID" to CTSS interface role,
	(2) define depending on the clientID the identity of the signature-creation key (keyID) to be used for the transaction log to CTSS interface role,
	(3) define the identity of the signature-creation key (keyID) to be used for the system log and audit logs to CTSS interface role,
	(4) increase by 1 the internally stored security attribute "transaction number" whenever a transaction is started to subjects in CTSS interface role,
	(5) modify the TD security attribute "transaction number" imported from the TD to none,
	(6) increase the security attribute "version number" of UCP after successful installation to CSP role.

PP application note 6: The refinements of FMT_MSA.1 are made in order to avoid iteration of the component.

6.1.1.5 FMT_MSA.3 Static attribute initialisation

Hierarchical to:	No other components.
Dependencies:	FMT_MSA.1 Management of security attributes
	FMT_SMR.1 Security roles
FMT_MSA.3.1	The TSF shall enforce ***the log message SFP and update SFP*** to provide ***restrictive*** default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2	The TSF shall allow the ***none*** to specify alternative initial values to override the default values when an object or information is created.

6.1.2 User identification and authentication

6.1.2.1 FIA_ATD.1 User attribute definition

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_ATD.1.1	The TSF shall maintain the following list of security attributes belonging to ***administrator:***
	(1) identity,
	(2) authentication reference data,
	(3) role
	and
	(a) security attribute identity, none[9] ***belonging to the ERS***
	(b) security attribute identity, none[10] ***belonging to the CSP.***

PP application note 7: The refinements distinguish between the sets of security attributes maintained for authenticated user Administrator, and the tested user ERS and CSP according to FTP_TEE.1. The security attributes are defined by user by Administrator according to FMT_MSA.1.

6.1.2.2 FMT_MTD.1/AD Management of TSF data - Authentication data

Hierarchical to:	No other components.
Dependencies:	FMT_SMR.1 Security roles
	FMT_SMF.1 Specification of Management Functions
FMT_MTD.1.1/AD	The TSF shall restrict the ability to
	(1) ***delete and create*** the ***authentication data record of all authorized users*** to ***administrator***.
	(2) ***modify the authentication reference data to the corresponding authorized user***.

6.1.2.3 FMT_MTD.3/PW Secure TSF data - Password

Hierarchical to:	No other components.
Dependencies:	FMT_MTD.1 Management of TSF data
FMT_MTD.3.1/PW	The TSF shall ensure that only secure values are accepted for ***passwords and enforce changing initial passwords after first successful authentication of the user to a different secure operational password.***

[9] [assignment: additional security attributes]

[10] [assignment: additional security attributes]

6.1.2.4 FIA_AFL.1 Authentication failure handling

Hierarchical to:	No other components.
Dependencies:	FIA_UAU.1 Timing of authentication
FIA_AFL.1.1	The TSF shall detect when **an administrator configurable positive integer within 1-15**[11] [12] unsuccessful authentication attempts occur related to **PIN-based authentication** [13].
FIA_AFL.1.2	When the defined number of unsuccessful authentication attempts has been **met**[14], the TSF shall **delay the next authentication attempt or block the authentication, configurable by the administrator**[15].

6.1.2.5 FIA_USB.1 User-subject binding

Hierarchical to:	No other components.
Dependencies:	FIA_ATD.1 User attribute definition
FIA_USB.1.1	The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: ***(1) identity,*** ***(2) role.***
FIA_USB.1.2	The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: ***the initial role of the user is unidentified user***.
FIA_USB.1.3	The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: ***(1) A subject is associated with attribute "identity" and "CTSS interface role" after the ERS is successfully tested according to FPT_TEE.1.*** ***(2) A subject is associated with attribute "identity" and "CSP role" after the CSP is successfully tested according to FPT_TEE.1.*** ***(3) A subject is associated with attribute "identity" and "administrator role" after successful authentication.***

6.1.2.6 FIA_UID.1 Timing of identification

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_UID.1.1	The TSF shall allow ***Self test according to FPT_TST.1*** on behalf of the user to be performed before the user is identified.
FIA_UID.1.2	The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

6.1.2.7 FIA_UAU.1 Timing of authentication

[11] [assignment: range of acceptable values]

[12] [selection: [assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]]

[13] [assignment: list of authentication events]

[14] [selection: met, surpassed]

[15] [assignment: list of actions]

Hierarchical to:	No other components.
Dependencies:	FIA_UID.1 Timing of identification
FIA_UAU.1.1	The TSF shall allow ***(1) self test according to FPT_TST.1,*** ***(2) testing of external entity ERS according to FPT_TEE.1 and start the subject CTSS interface component if testing was successful and the role CTSS interface component is activated,*** ***(3) testing of external entity CSP according to FPT_TEE.1 and start the subject CSP if testing was successful,*** ***(4) none,***[16] on behalf of the user to be performed before the user is authenticated.
FIA_UAU.1.2	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

6.1.2.8 FIA_UAU.5 Multiple authentication mechanisms

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_UAU.5.1	The TSF shall provide ***password authentication*** to support user authentication.
FIA_UAU.5.2	The TSF shall authenticate any user's claimed identity according to the ***rule that*** ***(1) password authentication shall be used for administrator,*** ***(2) none***[17]***.***

6.1.2.9 FIA_UAU.6 Re-authenticating

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_UAU.6.1	The TSF shall re-authenticate the user under the conditions ***power on or reset***.

6.1.3 User data protection

6.1.3.1 FDP_ACC.1/LM Subset access control – Access to Logging

Hierarchical to:	FDP_ACC.1 Subset access control
Dependencies:	FDP_ACF.1 Security attribute based access control
FDP_ACC.1.1/LM	The TSF shall enforce the ***log Message SFP*** on ***(1) subjects:*** ***(a) subject acting for CTSS interface component,*** ***(b) subject acting for CSP;*** ***(2) objects:*** ***(a) transaction data,*** ***(b) audit record,***

[16] [assignment: list of other TSF mediated actions]

[17] [assignment: additional rules describing how the multiple authentication mechanisms provide authentication]

(c) data-to-be-signed,

(d) protocolData with signature,

(e) log message;

(f) commands;

(3) operations:

(a) import,

(b) export.

6.1.3.2 FDP_ACF.1/LM Security attribute based access control – Access to TDS

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1/LM The TSF shall enforce the ***log Message SFP*** to objects based on the following:

(1) subjects:

(a) subject in CTSS interface role with security attribute activated or deactivated.

(b) subject in CSP role;

(2) objects:

(a) transaction data,

(b) audit record,

(c) data-to-be-signed,

(d) protocolData with signature,

(e) log message,

(f) commands.

FDP_ACF.1.2/LM The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

(1) A subject in activated CTSS interface role is allowed to

(a) import the transaction data from the CTSS interface component according to FDP_ITC.2/TD,

(b) import commands from activated CTSS interface component,

(c) export the DTBS of transaction log and system log to the CSP according to FDP_ETC.2/DTBS,

(d) import the protocolData with signature from the CSP according to FDP_ITC.2/TSS,

(e) export the transaction log and system log to the CTSS interface component according to FDP_ETC.2/LM.

(2) A subject in activated CTSS interface role is allowed to terminate the transaction after time limit defined according to FMT_MOF.1.1 clause (2) is reached.

(3) A subject in CSP role is allowed to import audit records from the CSP according to FDP_ITC.2/TSS and to export audit logs to the CTSS interface component according to FDP_ETC.2/LM.

FDP_ACF.1.3/LM	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules***:*** **None.**[18]
FDP_ACF.1.4/LM	The TSF shall explicitly deny access of subjects to objects based on the rules ***(1) a user in other role than CTSS interface role is not allowed to perform actions listed in FDP_ACF.1.2/LM clause (1) and (2).*** ***(2) a user in other role than CSP role is not allowed to perform actions listed in FDP_ACF.1.2/LM clause (3).***

6.1.3.3 FDP_ITC.2/TD Import of user data with security attributes – Transaction Data

Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] [FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path] FPT_TDC.1 Inter-TSF basic TSF data consistency
FDP_ITC.2.1/TD	The TSF shall enforce the ***log message SFP*** when importing ***transaction data*** controlled under the SFP, from outside of the TOE.
FDP_ITC.2.2/TD	The TSF shall use the security attributes associated with the imported ***transaction data.***
FDP_ITC.2.3/TD	The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the ***transaction data*** received.
FDP_ITC.2.4/TD	The TSF shall ensure that interpretation of the security attributes of the imported ***transaction data*** is as intended by the source of the user data.
FDP_ITC.2.5/TD	The TSF shall enforce the following rules when importing user data ***transaction data*** controlled under the SFP from outside of the TOE: ***(1) The TSF shall import the transaction data with the security attribute clientID if the clientID is in the set of accepted values according to FMT_MSA.1. If the clientID is not in the set of accepted values the TSF must not import the transaction data.*** ***(2) The TSF shall import the transaction data with the security attribute "type of the operation".*** ***(3) The transaction data shall be imported with the security attribute "transaction number" if the "type of the operation" is UpdateTransaction or FinishTransaction, and the transaction number meets a transaction number of an ongoing transaction.*** ***(4) The TSF shall import audit records from CSP.***

6.1.3.4 FDP_ETC.2/DTBS Export of user data with security attributes

Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]
FDP_ETC.2.1/DTBS	The TSF shall enforce the log message SFP when exporting ***data-to-be-signed,*** controlled under the SFP(s), ***to the CSP.***
FDP_ETC.2.2/DTBS	The TSF shall export the user data with the security attributes ***associated with data-to-be-signed.***

[18] [assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects]

FDP_ETC.2.3/DTBS	The TSF shall ensure that the security attributes, when exported outside the TOE, are unambiguously associated with the exported ***data-to-be-signed.***
FDP_ETC.2.4/DTBS	The TSF shall enforce the following rules when user data is exported from the TOE: ***(1) Data-to-be-signed shall be exported for generation of a log message with security attribute identifying the private signature key to be used by FDP_DAU.2/TS according to [PPC-CSP-TS-Au][PPC-CSP-TS-Au-Cl][PPC-CSPLight-TS-Au-Cl].***

6.1.3.5 FDP_ITC.2/TSS Import of user data with security attributes – Time stamp and signature

Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] [FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path] FPT_TDC.1 Inter-TSF basic TSF data consistency
FDP_ITC.2.1/TSS	The TSF shall enforce the ***log message SFP*** when importing ***protocolData with signature and audit records***, controlled under the SFP, from ***the CSP.***
FDP_ITC.2.2/TSS	The TSF shall use the security attributes associated with the imported user data.
FDP_ITC.2.3/TSS	The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the ***protocolData with signature and audit records*** received.
FDP_ITC.2.4/TSS	The TSF shall ensure that interpretation of the security attributes of the imported ***protocolData with signature and audit records*** is as intended by the source of the user data.
FDP_ITC.2.5/TSS	The TSF shall enforce the following rules when importing ***protocolData with signature and audit records*** controlled under the SFP from ***the CSP***: **None.**[19]

PP application note 8: The CSP shall generate and return to the TOE at least the signature counter of the used signature-creation key, the time stamp and the signatures for the data-to-be-signed exported by the TOE according to FDP_ETC.2/DTBS. The CSP shall generate time stamps according to FDP_DAU.2/TS using a time source according to FPT_STM.1, cf. [PPC-CSP-TS-Au][PPC-CSP-TS-Au-Cl][PPC-CSPLight-TS-Au-Cl]. Note, the TOE of this protection profile may use the CSP to provide time stamps by an administrator settable internal clock; cf. selection clause (4) in FPT_STM.1.1. If the CSP meets [TR SE] for the transaction logs, then the CSP returns a log message to the TOE. If the CSP generates the time stamp and signatures with a signature counter, then the TOE shall compile the log message according to [TR TSEA]. The signature counter and the time stamp of transaction logs and of audit data received as audit logs may be used to test the CSP according to FPT_TEE.1.

6.1.3.6 FDP_ETC.2/LM Export of user data with security attributes – Log messages

Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]
FDP_ETC.2.1/LM	The TSF shall enforce the ***log message SFP*** when exporting user data ***log message***, controlled under the SFP(s), ***to CTSS interface component***.
FDP_ETC.2.2/LM	The TSF shall export the user data with the user data's associated security attributes.

[19] [assignment: additional importation control rules]

FDP_ETC.2.3/LM The TSF shall ensure that the security attributes, when exported outside the TOE, are unambiguously associated with the exported user data.

FDP_ETC.2.4/LM The TSF shall enforce the following rules when user data is exported from the TOE: ***Log messages shall be exported with security attribute***

(1) transaction logs:

(a) transaction number of the ERS transaction and identifying the log messages which belongs to the transaction,

(b) signature counter of the private signature key used by FDP_DAU.2/TS according to [PPC-CSP-TS-Au][PPC-CSP-TS-Au-Cl][PPC-CSPLight-TS-Au-Cl] enumerating all log messages,

(c) type of the operation,

(d) time stamp when the log message was signed,

(e) keyID as hash value of the public key for verification of the signature,

(f) signature for verification of the authenticity of the certified data and protocol data.

(2) system logs:

(a) type of the operation or TSF security event

(b) signature counter of the private signature key used by FDP_DAU.2/TS according to [PPC-CSP-TS-Au][PPC-CSP-TS-Au-Cl][PPC-CSPLight-TS-Au-Cl] enumerating all log messages,

(c) time stamp when the log message was signed,

(d) keyID as hash value of the public key for verification of the signature,

(e) signature for verification of the authenticity of the certified data and protocol data.

(3) audit records of the CSP shall be exported unchanged as system logs to the CTSS interface component.

PP application note 9: The CTSS interface component does not implement any security functionality addressed in this PP and imports and stores log message received from the TOE as user data.

6.1.3.7 FPT_TDC.1 Inter-TSF basic TSF data consistency

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_TDC.1.1 The TSF shall provide the capability to consistently interpret

(1) clientID,

(2) type of the operation,

(3) transaction number,

(4) signature counter,

(5) time stamp,

(6) keyID as hash value of the public key

(7) signature

when shared between the TSF and another trusted IT product.

FPT_TDC.1.2 The TSF shall use ***[TR SE] and [TR TSEA]*** when interpreting the TSF data from another trusted IT product.

6.1.3.8 FMT_MSA.2 Secure security attributes

Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]
	FMT_MSA.1 Management of security attributes
	FMT_SMR.1 Security roles
FMT_MSA.2.1	The TSF shall ensure that only secure values are accepted for security attributes
	(1) transaction numbers building a strong increasing sequence without gaps,
	(2) time stamps of the log messages building a not decreasing sequence with consideration of adjustments of the CSP's time source.

PP application note 10: The rules are enforced by using certified functionality of the CSP.

6.1.3.9 FMT_MSA.4 Security attribute value inheritance

Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]
FMT_MSA.4.1	The TSF shall use the following rules to set the value of security attributes:
	(1) The TSF uses the security attribute clientID imported with transaction data to determine the signature-creation key that is used by FDP_DAU.2/TS with ECDSA in [PPC-CSP-TSAu][PPC-CSP-TS-Au-Cl][PPC-CSPLight-TS-Au-Cl] to sign the corresponding log message as defined according to FMT_MSA.1.
	(2) If the type of the operation of imported transaction data is StartTransaction then the last internally generated Transaction Number shall be increased by 1 and this value shall be assigned to the ongoing transaction and the Transaction log of imported Transaction Data.
	(3) If the Type of the Operation of imported Transaction Data is UpdateTransaction or FinishTransaction and meets the transaction number of an ongoing transaction then the transaction number of the imported transaction data shall be assigned to the protocol data of the transaction log.

6.1.4 Protection of the TSF

6.1.4.1 FPT_FLS.1 Failure with preservation of secure state

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_FLS.1.1	The TSF shall preserve a secure state when the following types of failures occur:
	(1) self test according to FPT_TST.1 fails,
	(2) test of ERS according to FPT_TEE.1 fails,
	(3) test of CSP according to FPT_TEE.1 fails.
	The TSF shall exit the secure state only if the self-test, the test of the ERS and the test of the CSP are passed.

PP application note 11: The self-test according to FPT_TST.1 and test of external entities according to FPT_TEE.1 cause the secure state if the self-test or the tests fail. The exit of the secure state requires all conditions listed in the refinement being fulfilled.

6.1.4.2 FPT_TEE.1 Testing of external entities

Hierarchical to:	No other components.

Dependencies:	No dependencies.
FPT_TEE.1.1	The TSF shall run a suite of tests ***during start-up, periodically during normal operation, user initiated shutdown and before exiting the secure state according to FPT_FLS.1*** to check the fulfillment of ***(1) ERS identity,*** **none**[20] ***and*** ***(2) CSP identity,*** **none**[21]***.*** ***The tests include the identification of the TOE to the tested device.***
FPT_TEE.1.2	If the test fails, the TSF shall ***enter the secure state according to FPT_FLS.1,*** **none additional action.**[22]

PP application note 12: The administrator may by able to define the actions in FPT_TEE.1 according to FMT_MOF.1.1 (5). In case of a failure, additional actions may e.g. include reading the stored audit logs. The suite of tests determine whether the configured CSP is available for the TOE and log messages can be signed. The TOE may use the signature counter and time stamps received from the CSP to test it. The signature counter shall increase strong monotonically without gaps because any gap may indicate unauthorized signature-creation. The tests of the CSP should allow the CSP to identify the TOE as user of the CSP, cf. FIA_UID.1.1 clause (2) in [PP CSP][PP CSPLight]. Please refer for further explanations to the user notes and evaluator notes in CC part 2 [CC_2], Chapter J.12

6.1.4.3 FPT_TST.1 TSF testing

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_TST.1.1	The TSF shall run a suite of self tests ***during initial start-up, at the request of the authorised user, periodically during normal operation and before exiting the secure state according to FPT_FLS.1*** to demonstrate the correct operation of **parts of TSF.**
FPT_TST.1.2	The TSF shall provide authorised users with the capability to verify the integrity of ***TSF data.***
FPT_TST.1.3	The TSF shall provide authorised users with the capability to verify the integrity of ***TSF implementation***.

PP application note 13: The security attribute “version number” of the UCP is part of the TSF data. During TSF testing, the consistency of the version number has to be checked to detect upgrades or attempted downgrades of the installed code of the TOE. In case of a detected change of the version number, the TOE must follow the UCP SFP and log the events according to FAU_GEN.1/SYS.

6.1.5 Security Audit

6.1.5.1 FAU_GEN.1/SYS Audit data generation – System Log

Hierarchical to:	No other components.
Dependencies:	FPT_STM.1 Reliable time stamps

[20] [assignment: list of properties of the ERS]

[21] [assignment: list of properties of the CSP]

[22] [selection: none additional action, [assignment: additional action(s)]

FAU_GEN.1.1/SYS The TSF shall be able to generate an audit record of the following auditable events:

a) start-up and shutdown of the audit functions;

b) all auditable events for the ***not specified*** level of audit; and

c) ***other auditable events***

(1) system operation commands as specified in [TR SE], Appendix A,

(2) authentication failure handling (FIA_AFL.1): the reaching of the threshold for the unsuccessful authentication attempts with claimed Identity of the user,

(3) failure with preservation of secure state (FPT_FLS.1): entering and exiting secure state,

(4) setting of the version number of the UCP and upgrade of stored data,

(5) all auditable according to [Klarstellungen][23].

FAU_GEN.1.2/SYS The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the ST, **none**[24].

PP application note 14: The security relevant events that have to be logged according to FAU_GEN.1/SYS are part of the system log.

6.1.5.2 FMT_MTD.1/SYSCTSS Management of TSF data – System log – CTSS Interface Component

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1/SYSCTSS The TSF shall restrict the ability to

(1) ***manual export,***

(2) ***clear after manual export***,

the ***system logs*** to ***CTSS Interface Component***.

6.1.5.3 FMT_MTD.1/SYSAdmin Management of TSF data – System log -Administrator

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1/SYSAdmin The TSF shall restrict the ability to

(1) select audited events in FAU_GEN.1/SYS,

(2) define the number of audit records causing automatic export and clearing of exported audit records according to FAU_STG.3.1/SYS clause (1),

(3) define the percentage of storage capacity of audit records if actions are assigned in FAU_STG.3.1/SYS clause (2)

the ***system logs*** to ***Administrator***.

[23] [assignment: additional specifically defined auditable events]

[24] [assignment: other audit relevant information]

6.1.5.4 FAU_STG.1/SYS Protected audit trail storage – System log

Hierarchical to:	No other components.
Dependencies:	FAU_GEN.1 Audit data generation
FAU_STG.1.1/SYS	The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.
FAU_STG.1.2/SYS	The TSF shall be able to ***prevent*** unauthorised modifications to the stored audit records in the audit trail.

6.1.5.5 FAU_STG.3/SYS Action in Case of Possible Audit Data Loss – System log

Hierarchical to:	No other components.
Dependencies:	FAU_STG.1 Protected audit trail storage
FAU_STG.3.1/SYS	The TSF shall (1) ***automatically export audit trails and clear automatically exported audit records*** if the audit trail exceeds ***an Administrator defined number of audit records within 1[25].*** ***(2) No actions[26] if the audit trail exceeds an Administrator settable percentage of storage capacity.***

PP application note 15: The ST writer shall perform the open operations in FAU_STG.3.1/SYS element. If the number of audit records in clause (1) is set to 1 then the TSF export each audit record automatically. If the number of audit records in clause (1) is set higher than maximum number of audit records in the audit trail then the TSF does not export audit records automatically. The assignment of clause (2) may be "no actions" if an appropriate number of audit records is assigned in clause (1).

Application note 16: The automatic export shall prevent loss of internal audit data due to storage constraints, by protecting the audit data and storing the signed and timestamped data in the CTSS interface component, i.e. outside the TOE.

6.1.6 Code Update Package import

6.1.6.1 FDP_ACC.1/UCP Subset access control – Use of Update Code Package

Hierarchical to:	FDP_ACC.1 Subset access control
Dependencies:	FDP_ACF.1 Security attribute based access control
FDP_ACC.1.1/UCP	The TSF shall enforce the ***Update SFP*** on ***(1) subjects: CSP role;*** ***(2) objects: stored data;*** ***(3) operations: upgrade.***

6.1.6.2 FDP_ACF.1/UCP Security attribute based access control – Import Update Code Package

Hierarchical to:	No other components.
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation

[25] [assignment: pre-defined range]

[26] [assignment: actions to be taken in case of possible audit storage failure]

FDP_ACF.1.1/UCP	The TSF shall enforce the ***Update SFP*** to objects based on the following: ***(1) subjects: CSP role;*** ***(2) objects: update code package with security attributes version number.***
FDP_ACF.1.2/UCP	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: ***(1) CSP role is allowed to upgrade the stored data if*** ***(a) the digital signature of the UCP generated by the issuer is successfully verified by the SMAERS platform.***
FDP_ACF.1.3/UCP	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **none.**[27]
FDP_ACF.1.4/UCP	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: ***(1) a CSP role is not allowed to upgrade the stored data if the verification of digital signature of the UCP by means of the SMAERS platform fails;*** ***(2)*** **None.**[28]

PP application note 17: The CSP role should be allowed to apply the stored update code package if the version number of the update code package is higher than the version number of the TSF. The execution of UCP is outside the TSF-mediated functionality of the PP on hand.

6.1.6.3 FDP_ETC.2/UCP_UD Export of user data with security attributes – User Data

Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]
FDP_ETC.2.1/UCP_UD	The TSF shall enforce the ***update SFP*** when exporting user data, controlled under the SFP(s), outside of the TOE ***to the storage of the platform.***
FDP_ETC.2.2/ UCP_UD	The TSF shall export the user data with the user data's associated security attributes.
FDP_ETC.2.3/ UCP_UD	The TSF shall ensure that the security attributes, when exported outside the TOE, are unambiguously associated with the exported user data.
FDP_ETC.2.4/ UCP_UD	The TSF shall enforce the following rules when user data is exported from the TOE: **None**[29] .

6.1.6.4 FDP_ITC.2/UCP_UD Import of user data with security attributes – Update Code Package

Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] [FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path] FPT_TDC.1 Inter-TSF basic TSF data consistency
FDP_ITC.2.1/UCP_UD	The TSF shall enforce the ***update SFP*** when importing user data, controlled under the SFP, from ***the storage of the platform***.

[27] [assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects]

[28] [assignment: other rules, based on security attributes, that explicitly deny access of subjects to objects]

[29] [assignment: additional exportation control rules]

FDP_ITC.2.2/UCP_UD	The TSF shall use the security attributes associated with the imported user data.
FDP_ITC.2.3/UCP_UD	The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the user data received.
FDP_ITC.2.4/UCP_UD	The TSF shall ensure that interpretation of the security attributes of the imported user data is as intended by the source of the user data.
FDP_ITC.2.5/UCP_UD	The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: **None**[30]**.**

6.1.6.5 FDP_RIP.1/UCP Subset residual information protection

Hierarchical to:	No other components
Dependencies:	No dependencies.
FDP_RIP.1.1/UCP	The TSF shall ensure that any previous information content of a resource is made unavailable upon the ***deallocation of the resource after successful upgrade of the stored data*** the following objects: ***previous code and data.***

6.2 Security assurance requirements

The PP requires the TOE to be evaluated according to EAL2 augmented with ALC_CMS.3 (Implementation representation CM coverage) and ALC_LCD.1 (Developer-Defined Lifecycle Model), and with specific refinements on ALC_CMS.3, ADV_ARC.1 and ATE_IND.2.

6.2.1 Assurance Refinements

Refinement on ALC_CMS.3.1C:

The implementation representation listed shall comprise the implementation representation of the TOE defining the TSF to a level of detail such that the compliance of the TOE and TSF to the requirements imposed by the platform guidances on which the TOE is designed to run on, can be verified by that evidence.

Refinement on ADV_ARC.1.3D:

The security guidance documentation of each platform (hardware and software platform and operating system) on which the TOE is designed to run shall be provided in addition.

Refinement on ADV_ARC.1.1C to 1.5C:

The security architecture description shall include an assessment how each single security requirement imposed by the platform documentation (guidance documentation and if available evaluation or certification results) has been followed in the TOE design and implementation concept.

Examples for such security requirements could include but are not limited to:

- ***Dedicated library calls: Dedicated calls protecting against attacks may be provided by the platform for cryptographic operation. For example, dedicated calls implement operations that are hardened against timing side channel attacks, while others execute faster, but are not hardened. The platformguidance may require such library calls to be used.***
- ***Key usage limitations: Key usage above a certain limit may reveal side channel information which can then be exploited. The implementation must ensure that the key usage limit is adhered to.***

[30] [assignment: additional importation control rules]

- ***Dedicated calls to ensure a correct program flow are provided (i.e. for boolean verification calls) to ensure protection against attacks that disturb the execution flow. Such library calls must be made use of in critical operations.***
- ***Dedicated library calls are provided for the secure generation of cryptographic random numbers. Other random number generation functionality is present, but is not suitable to generate cryptographic random numbers. It must be ensured that correct random number generation library calls are used.***

Refinement on ADV_ARC.1.1E:

The evaluators task includes to check consistency of the requirements considered in the architectural description against those outlined in the platform documentation.

Refinement on ATE_IND.2.1D:

Providing the TOE for testing shall include in addition the implementation representation of the TOE as defined by ALC_CMS.3.

Refinement of ATE_IND.2.2C:

The resources provided shall include additionally appropriate tools or access to the TOE development environment in order to enable the evaluator to perform source code review most efficiently.

Refinement of ATE_IND.2.3E:

The evaluators test activities shall include a verification of the TOE implementation representation provided in order to confirm code compliance of the TOE implementation representation to the security guidance of the hardware platform and operating system and libraries which the TOE/TSF is intended to be run on. Therefore, the evaluator shall assess and verify that all platform guidance requirements are met and indicate possible vulnerabilities to the AVA evaluation activity for the TOE for further consideration.

6.3 Security requirements rationale

6.3.1 Dependency rationale

This chapter demonstrates that each dependency of the security requirements defined in chapter 6.1 is either satisfied, or justifies the dependency not being satisfied.

SFR	Dependencies of the SFR	SFR components
FAU_GEN.1/SYS	FPT_STM.1 Reliable time stamps	FPT_STM.1 provided by the CSP PP Module Time Stamp Service and Audit
FAU_STG.1/SYS	FAU_GEN.1 Audit data generation	FAU_GEN.1/SYS
FAU_STG.3/SYS	FAU_STG.1 Protected audit trail storage	FAU_STG.1/SYS
FDP_ACC.1/LM	FDP_ACF.1 Security attribute based access control	FDP_ACF.1/LM
FDP_ACC.1/UCP	FDP_ACF.1 Security attribute based access control	FDP_ACF.1/UCP
FDP_ACF.1/LM	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation	FDP_ACC.1/LM, FMT_MSA.3

SFR	Dependencies of the SFR	SFR components
FDP_ACF.1/UCP	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation	FDP_ACC.1/UCP, FMT_MSA.3
FDP_ETC.2/DTBS	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]	FDP_ACC.1/LM
FDP_ETC.2/LM	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]	FDP_ACC.1/LM
FDP_ETC.2/UCP_UD	FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]	FDP_ACC.1/UCP
FDP_ITC.2/TD	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] [FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path] FPT_TDC.1 Inter-TSF basic TSF data consistency	FDP_ACC.1/LM Dependency on FTP_ITC.1 or FTP_TRP.1 is not fulfilled because secure import is ensured by OE.SecOEnv. FPT_TDC.1
FDP_ITC.2/TSS	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] [FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path] FPT_TDC.1 Inter-TSF basic TSF data consistency	FDP_ACC.1/LM Dependency on FTP_ITC.1 or FTP_TRP.1 is not fulfilled because secure import is ensured by OE.SecCommCSP in case of platform architecture.
FDP_ITC.2/UCP_UD	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] [FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path] FPT_TDC.1 Inter-TSF basic TSF data consistency	FDP_ACC.1/UCP, FTP_ITC.1 is not included for UCP transfer but FDP_ACC.1/UCP ensure integrity and confidentiality of UCP, FPT_TDC.1 is not included because CSP uses the security attributes of UCP
FDP_RIP.1/UCP	No dependencies	
FIA_AFL.1	FIA_UAU.1 Timing of authentication	FIA_UAU.1
FIA_ATD.1	No dependencies	
FIA_UAU.1	FIA_UID.1 Timing of identification	FIA_UID.1
FIA_UAU.5	No dependencies	
FIA_UAU.6	No dependencies	
FIA_UID.1	No dependencies	
FIA_USB.1	FIA_ATD.1 User attribute definition	FIA_ATD.1
FMT_MOF.1	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FMT_SMF.1, FMT_SMR.1

SFR	Dependencies of the SFR	SFR components
FMT_MSA.1	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FDP_ACC.1/LM, FDP_ACC.1/UCP FMT_SMR.1 FMT_SMF.1
FMT_MSA.2	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles	FDP_ACC.1/LM, FDP_ACC.1/UCP, FMT_MSA.1, FMT_SMR.1
FMT_MSA.3	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles	FMT_MSA.1, FMT_SMR.1
FMT_MSA.4	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]	FDP_ACC.1/LM
FMT_MTD.1/AD	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FMT_SMF.1, FMT_SMR.1
FMT_MTD.1/SYSCTSS	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FMT_SMF.1, FMT_SMR.1
FMT_MTD.1/SYSAdmin	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FMT_SMF.1, FMT_SMR.1
FMT_MTD.3/PW	FMT_MTD.1 Management of TSF data	FMT_MTD.1/AD
FMT_SMF.1	No dependencies	
FMT_SMR.1	FIA_UID.1 Timing of identification	FIA_UID.1
FPT_TDC.1	No dependencies	
FPT_FLS.1	No dependencies	
FPT_TEE.1	No dependencies	
FPT_TST.1	No dependencies	

Table 3: Dependency rationale

6.3.2 Security functional requirements rationale

The tables trace each SFR defined in chapter 6.1 back to the security objectives for the TOE.

	O.GenLM	O.ImpExp	O.IAA	O.SecMan	O.TEE	O.TST	O.ImpExpUCP
FAU_GEN.1/SYS	x						
FAU_STG.1/SYS	x						
FAU_STG.3/SYS	x						
FDP_ACC.1/LM	x	x					
FDP_ACC.1/UCP						x	
FDP_ACF.1/LM	x	x					
FDP_ACF.1/UCP						x	
FDP_ETC.2/DTBS	x						
FDP_ETC.2/LM		x					
FDP_ITC.2/TSS	x						
FDP_ITC.2/TD	x	x					
FDP_ITC.2/UCP_UD						x	x
FDP_ETC.2/UCP_UD						x	x
FDP_RIP.1/UCP						x	
FIA_AFL.1			x				
FIA_ATD.1			x		x		
FIA_UAU.1					x		
FIA_UAU.5			x				
FIA_UAU.6			x				
FIA_UID.1					x		
FIA_USB.1			x				
FMT_MOF.1	x		x	x	x		
FMT_MSA.1	x			x	x		
FMT_MSA.2	x			x			
FMT_MSA.3	x			x			
FMT_MSA.4	x	x		x			
FMT_MTD.1/AD			x	x			
FMT_MTD.1/SYSCTSS	x						
FMT_MTD.1/SYSAdmin	x						
FMT_MTD.3/PW			x	x			
FMT_SMF.1	x	x		x			
FMT_SMR.1	x	x		x	x		

	O.GenLM	O.ImpExp	O.IAA	O.SecMan	O.TEE	O.TST	O.ImpExpUCP
FPT_TDC.1	x	x					
FPT_FLS.1					x	x	
FPT_TEE.1					x	x	
FPT_TST.1						x	

Table 4: Security functional requirements rationale

The following part of this chapter demonstrates that the SFRs meet all security objectives for the TOE.

The security objective for the TOE O.GenLM Generation of Log Messages is met by the following SFR:

- The SFR FDP_ACC.1/LM and FDP_ACF.1/LM require access control of import of TD and signatures, export of DTBS and log messages for roles defined by FMT_SMR.1.
- The SFR FDP_ITC.2/TD and FDP_ITC.2/TSS requires the TSF to import transaction data from CTSS interface component, audit records, time stamps, signature counter and signatures from CSP to generate log messages.
- The SFR FDP_ETC.2/DTBS requires the TSF to export data-to-be-signed to the CSP for time stamping and signature generation.
- The SFR FMT_MSA.1, clause (3) prevents the manipulation of the transaction number.
- The SFR FMT_MSA.2 ensures that the security attributes of a log message are generated in a way that the log message builds a valid transaction.
- The SFR FMT_MSA.3 ensures restrictive security attributes of a log message as defined, and prevents alternative initial values of the security attributes of a log message.
- The SFR FMT_MSA.4 describes the generation of security attributes which are included in a log message.
- The SFR FMT_MOF.1 clause (2), describes the behaviour of FMT_MSA.4 for keyID in a log message.
- The SFR FMT_MOF.1, FMT_MTD.3/PW, FMT_MSA.3, FMT_MSA.4 defined for SFR FDP_ACC.1/LM and FDP_ACF.1/LM are listed in SFR FMT_SMF.1.
- The SFR FPT_TDC.1 ensures that the security attributes of the imported transaction data and of the exported log messages are correctly interpreted.
- The SFR FAU_GEN.1/SYS, FMT_MTD.1/SYSCTSS, FMT_MTD.1/SYSAdmin, FAU_STG.1/SYS, FAU_STG.3/SYS decribes the generation and management of system logs.

The security objective for the TOE O.ImpExp Import of Transaction Data from and Export of Log message to CTSS Interface Component is met by the following SFR:

- The SFR FDP_ACC.1/LM and FDP_ACF.1/LM require access control on the import of transaction data; and export of log messages to the CTSS interface component for roles defined by FMT_SMR.1.
- The SFR FDP_ITC.2/TD requires the TSF to import transaction data with security attributes in order to determine the security attributes of log messages according to FMT_MSA.4.

- The SFR FDP_ETC.2/LM requires the export of log messages with security attributes defined by FMT_MSA.4 to the CTSS interface component for generation of receipts and verification of log messages.
- The SFR FPT_TDC.1 ensures that the security attributes imported with transaction data and exported with log messages are correctly interpreted.

The security objective for the TOE O.IAA Authentication of Administrators is met by the following SFR:

- Administrator and CSP are requested to authenticate themselves according to FIA_UAU.5.
- The SFR FIA_UAU.5 defines the authentication mechanisms supported by the TSF.
- The SFR FMT_MOF.1.1, clause (1) defines the rule that additional authentication (except for the administrator itself) may be enabled and disabled by an administrator.
- The SFR FIA_UAU.6 defines the condition for re-authentication.
- The SFR FIA_AFL.1 defines required actions if password authentication fails.
- The SFR FIA_ATD.1 defines the security attributes of users known to the TSF and the SFR FIA_USB.1 requires binding these security attributes to successfully authenticated users.
- The SFR FMT_MTD.1/AD and FMT_MTD.3/PW require the TSF to manage authentication data of users.

The security objective for the TOE O.SecMan Security Management is met by the following SFRs:

- The SFR FMT_SMR.1 defines the roles known to TSF and requires the TSF to associate users with these roles.
- The SFR FMT_SMF.1 lists the management functions as management of functions FMT_MOF.1, management of TSF data FMT_MTD.1/AD and FMT_MTD.3/PW, and management of security attributes FMT_MSA.1, FMT_MSA.2, FMT_MSA.3 and FMT_MSA.4.
- The SFR FMT_MOF.1 restricts the ability to modify, enable, disable, determine the behaviour of and modify the behaviour of security functions to an administrator.
- The SFR FMT_MTD.1/AD and FMT_MTD.3/PW requires the TSF to manage authentication data of users.
- The SFR FMT_MSA.1 and FMT_MSA.3 describes the requirements for restrictive security attributes and limits the management of security attributes for the SFP Log Message and Update.
- The SFR FMT_MSA.2 and FMT_MSA.4 define requirements for the generation of security attributes of TDSs and TDSSs including the security attribute time stamp.
- The SFR FMT_MSA.4 prevents management of the transaction numbers.

The security objective for the TOE O.TEE Test of External Entities is met directly by the SFR FPT_TEE.1. The SFR FMT_MOF.1, clause (5), restricts the definition and modification of the behaviour of FPT_TEE.1 to the administrator. The O.TEE Test of External Entities is furthermore met by the following SFRs:

- The SFR FMT_SMR.1 lists the roles known to the TSF, where subject CTSS interface component is automatically started and identified only.
- The SFR FIA_UID.1 defines the self-test as the only TSF mediated action allowed before users and subjects are identified.
- The SFR FIA_UAU.1 defines the TSF mediated action allowed before users and subjects are authenticated.
- The subject CTSS interface component is allowed to perform automatically TSF mediated actions according to FPT_TST.1 and FPT_TEE.1 before users are authenticated.

- The SFR FIA_ATD.1 defines the security attribute identity for the ERS and the CSP tested by FPT_TEE.1. If any test fails, the TSF enters a secure state according to FPT_FLS.1.

The security objective for the TOE O.TST Self-Test is met by the following SFRs:

- The SFR FPT_TST.1 requires the TSF to perform self-tests and FPT_FLS.1 requires the TSF to enter a secure state if one of the self-tests fails.
- The SFR FPT_FLS.1 requires the TSF to enter a secure state if the self-test fails, or the test of the electronic record-keeping system fails, or the test of cryptographic service provider fails.
- The SFR FPT_TEE.1 requires the TSF to enter the secure state according to FPT_FLS.1 if the test of the CTSS interface component or the CSP fails.
- The SFR FDP_ACC.1/UCP and FDP_ACF.1/UCP requires the TSF to provide access control to enforce the update SFP. The SFR FMT_MSA.1 prevents the modification of security attributes “version number” of the UCP.
- The SFR FDP_RIP.1/UCP requires the TSF to remove the received UCP after unsuccessful verification of its authenticity. The verification must be done by means of the platform.

The security objective for the TOE O.ImpExpUCP Secure Import and Export of User Data is directly met by the SFR FDP_ITC.2/UCP_UD and FDP_ETC.2/UCP_UD that requires the TSF to export and import user data during an update process.

6.3.3 Security Assurance Requirements Rationale

Developers and users require for the TOE a low to moderate level of independently assured security in the absence of ready availability of the complete development record.

EAL2 was chosen because it provides assurance by a full security target and an analysis of the SFRs in that ST, using a functional and interface specification, guidance documentation and a basic description of the architecture of the TOE to understand the security behaviour. The analysis is supported by independent testing of the TSF, evidence of developer testing based on the functional specification, selective independent confirmation of the developer test results, and a vulnerability analysis – based upon the functional specification, TOE design, security architecture description and guidance evidence provided – demonstrating resistance to penetration attackers with a basic attack potential. EAL2 also provides assurance through the use of a configuration management system and evidence of secure delivery procedures.

ALC_CMS.3 has been augmented to include the implementation representation as needed for ADV_ARC and ATE_IND refinements, and to get evidence that the implementation representation provided is the one of the TOE. This means that the implementation representation is part of the configuration list.

The security target shall describe the complete life cycle of the TOE, including details necessary for the understanding of the interaction with and configuration of the CSP. Hence, ALC_LCD.1 has been augmented such that the lifecycle of the TOE is defined by the developer and thus made explicit.

For getting confidence that the platform of the TOE (operational environment) is used by the TOE in a way that the requirements on security as outlined in the platform documentation (guidance documentation and if available evaluation or certification results) have been followed in the TOE design and implementation, refinements of ADV_ARC, ATE_IND and ALC_CMS have been defined.

The goal is to ensure that the TOE implementation does not include obvious vulnerabilities caused by incorrect use of the platform, and that all relevant platform guidance requirements are adhered to. Therefore, only those requirements have to be considered that are related to the TOE functionality and security claims of the security target of the TOE.

The refinement of ADV_ARC ensures that the developer outlines how she has considered the requirements from the platform within his TOE security architecture and design concept. The evaluators task is to check consistency of the requirements considered against those outlined in the platform documentation.

As a second step of verification that the relevant platform requirements have been considered correctly, the independent evaluator activity at ATE_IND has been refined. The evaluator has to perform a specific „source code review“, by means of cross checking the requirements from the platform to the implementation representation of the TOE by examining the implementation representation of the TOE using appropriate tools and the evidence from ADV_ARC.

7 Package Trusted Channel between TOE and CSP

This chapter of the protection profile has been omitted, since the TOE of this security target are not physically separated components and the operational environment can ensure the integrity of the communication between the TOE and the CSP.

8 TOE summary specification (ASE_TSS)

8.1 TOE Security Functionality

8.1.1 TSF_Management: Management of the security functionality

This security functionality manages the configuration of the TOE and its security functions. During personalization, it manages instantiation and initial creation of objects. It provides default values and handles dynamic configuration data. This security functionality ensures that all security relevant data is stored in a secure way by using certified functions of the dedicated platform.

In operational life cycle state this TSF manages the configuration functions of the Administrator, CTSS Administrator and Time Administrator, e.g., setting the system time and mapping ERS to Key.

8.1.2 TSF_Log: Handling of log data and signature functionality

This Security Functionality manages the signature functionality and the according system and transaction logging. It ensures that the needed types of data to be signed are present and passes them in the expected form to the CSP for signature creation. Furthermore, it guarantees that the received signature and further security attributes are correctly exported.

8.1.3 TSF_Auth: Authentication protocols

This security functionality uses different authentication mechanisms to differentiate identities and roles. This includes, e.g., password authentication for users as well as CSP and CTSS role authentication after a successful self test. Additionally it manages reauthentication of these roles. Within the TOE, TSF_Auth is implemented using the authentication mechanisms provided by TSF_CSP.

8.1.4 TSF_CSP: Cryptographic service provider

The cryptography-based security functionality of the TOE is provided by the cryptographic service provider. This includes authentication methods TSF_Auth relies on, as well as signature creation needed by TSF_Log. This TSF represents the dedicated platform cryptovision CSP and implement all cryptographic functions needed by the TOE. Please note that this functionality is designated as “TSF” although the CSP is not a part of the TOE.

8.1.5 TSF_Update: Update functionality and according management

TSF_Update comprises the functionality that is used to provide updates of the TOE. It is based on the Global Platform mechanisms of the CSP platform [GP_CIC].

8.2 TOE summary specification rationale

This summary specification shows that the TSF and assurance measures are appropriateto fulfill the TOE security requirements.

Each TOE security functional requirement is implemented by at least one security functionality. The mapping of TOE Security Requirements and TOE Security Functionalities is given in the following table. If iterations of a TOE security requirement are covered by the same TOE security functionality the mapping will appear only once. The description of the TSF is given in section 8.1.

	TSF_Management	TSF_Log	TSF_Auth	TSF_CSP	TSF_Update
FAU_GEN.1/SYS	x	x	x	x	
FAU_STG.1/SYS				x	
FAU_STG.3/SYS	x	x	x	x	
FDP_ACC.1/LM	x	x	x	x	
FDP_ACC.1/UCP		x		x	x
FDP_ACF.1/LM	x	x	x	x	
FDP_ACF.1/UCP		x		x	x
FDP_ETC.2/DTBS	x	x	x	x	
FDP_ETC.2/LM	x	x	x	x	
FDP_ITC.2/TSS	x	x	x	x	
FDP_ITC.2/TD	x	x	x	x	
FDP_ITC.2/UCP_UD		x		x	x
FDP_ETC.2/UCP_UD		x		x	x
FDP_RIP.1/UCP		x		x	x
FIA_AFL.1	x	x	x	x	
FIA_ATD.1	x	x	x	x	
FIA_UAU.1	x	x	x	x	
FIA_UAU.5	x	x	x	x	
FIA_UAU.6	x		x	x	
FIA_UID.1	x	x	x	x	
FIA_USB.1	x	x	x	x	
FMT_MOF.1	x	x	x	x	
FMT_MSA.1	x	x	x	x	
FMT_MSA.2	x	x	x	x	
FMT_MSA.3	x				
FMT_MSA.4		x	x	x	
FMT_MTD.1/AD	x		x	x	
FMT_MTD.1/SYSCTSS		x	x	x	
FMT_MTD.1/SYSAdmin	x	x	x	x	
FMT_MTD.3/PW	x	x	x	x	
FMT_SMF.1	x	x	x	x	
FMT_SMR.1	x	x	x	x	

	TSF_Management	TSF_Log	TSF_Auth	TSF_CSP	TSF_Update
FPT_TDC.1	x	x	x	x	
FPT_FLS.1			x	x	
FPT_TEE.1	x			x	
FPT_TST.1	x			x	

Table 5: SFR and TSF mapping

- FAU_GEN.1/SYS requires that the TSF shall be able to generate an audit record for specified auditable events, and that the TSF shall record within each audit record among others at least the following information: date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event. This is realized by TSF_Log supported by TSF_Management and TSF_Auth based on the security functionality of the CSP platform (TSF_CSP).
- FAU_STG.1/SYS requires that the TSF shall protect the stored audit records in the audit trail from unauthorised deletion, and that the TSF shall be able to prevent unauthorised modifications to the stored audit records in the audit trail. This is realized by the security functionality of the CSP platform (TSF_CSP).
- FAU_STG.3/SYS requires that the TSF shall automatically export audit trails and clear automatically exported audit records if the audit trail exceeds an Administrator defined number of audit records, and that measures shall be taken if the audit trail exceeds an Administrator settable percentage of storage capacity. This is realized by TSF_Log supported by TSF_Management and TSF_Auth based on the security functionality of the CSP platform (TSF_CSP).
- FDP_ACC.1/LM requires that the TSF shall enforce the Log Message SFP on (1) subjects: (a) subject acting for CTSS interface component, (b) subject acting for CSP; (2) objects: (a) Transaction Data, (b) Audit record, (c) Data To Be Signed, (d) protocolData with Signature, (e) Log message; (3) operations: (a) import, (b) export. This is realized by TSF_Management, TSF_Log, TSF_Auth based on security functionality provided by the CSP platform (TSF_CSP).
- FDP_ACC.1/UCP requires that the TSF shall enforce the Update SFP on (1) subjects: Administrator; (2) objects: Update Code Package; (3) operations: import, decrypt. This is realized by TSF_Update supported by TSF_Log based on security functionality provided by the CSP platform (TSF_CSP).
- FDP_ACF.1/LM: FDP_ACF.1.1/LM requires that the TSF shall enforce the Log Message SFP to objects based on the following: (1) subjects: (a) subject in CTSS interface role with security attribute activated or deactivated. (b) subject in CSP role; (2) objects: (a) Transaction Data, (b) Audit record, (c) Data To Be Signed, (d) protocolData with Signature, (e) Log message. This is realized by TSF_Management, TSF_Log, TSF_Auth based on security functionality provided by the CSP platform (TSF_CSP).

- FDP_ACF.1/UCP: FDP_ACF.1.1/UCP requires that the TSF shall enforce the Update SFP to objects based on the following: (1) subjects: Administrator; (2) objects: Update Code Package with security attributes Issuer and Signature. FDP_ACF.1.2/UCP requires that the TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: (1) Administrator is allowed to import and store received Update Code Package if (a) the digital signature of the UCP generated by the Issuer is successful verified by the CSP and (b) the verified UCP is deciphered by means of CSP. FDP_ACF.1.3/UCP requires that the TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none. FDP_ACF.1.4/UCP requires that the TSF shall explicitly deny access of subjects to objects based on the following additional rules: (1) Administrator is not allowed to import received Update Code Package if verification of digital signature by means of CSP fails; (2) None. This is realized by TSF_Update supported by TSF_Log based on security functionality provided by the CSP platform (TSF_CSP).
- FDP_ETC.2/DTBS: FDP_ETC.2.1/DTBS requires that the TSF shall enforce the Log message SFP when exporting Data To Be Signed, controlled under the SFP(s), to CSP. FDP_ETC.2.2/DTBS requires that the TSF shall export the user data with the security attributes associated with Data To Be Signed. FDP_ETC.2.3/DTBS requires that the TSF shall ensure that the security attributes, when exported outside the TOE, are unambiguously associated with the exported Data To Be Signed. FDP_ETC.2.4/DTBS requires that the TSF shall enforce the following rules when user data is exported from the TOE: (1) Data To Be Signed shall be exported for generation of a Log message with security attribute identifying the private signature key to be used by FDP_DAU.2/TS according to [PPC-CSP-TS-Au]. This is realized by TSF_Management, TSF_Log, TSF_Auth based on security functionality provided by the CSP platform (TSF_CSP).
- FDP_ETC.2/LM: FDP_ETC.2.1/LM requires that the TSF shall enforce the Log message SFP when exporting user data Log message, controlled under the SFP(s), to CTSS interface component. FDP_ETC.2.2/LM requires that the TSF shall export the user data with the user data's associated security attributes. FDP_ETC.2.3/LM requires that the TSF shall ensure that the security attributes, when exported outside the TOE, are unambiguously associated with the exported user data. FDP_ETC.2.4/LM requires that the TSF shall enforce the following rules when user data is exported from the TOE: Log messages shall be exported with security attribute (1) Transaction logs: (a) Transaction number of the ERS transaction and identifying the Log messages which belongs to the transaction, (b) Signature Counter of the private signature key used by FDP_DAU.2/TS according to [PPC-CSP-TS-Au] enumerating all Log messages, (c) Type of the Operation, (d) Time stamp when the Log message was signed, (e) Serial Number as hash value of the public key for verification of the Signature, (f) Signature for verification of the authenticity of the certified data and protocol data. (2) Audit records of the CSP shall be exported unchanged as system logs to the CTSS interface component. This is realized by TSF_Management, TSF_Log, TSF_Auth based on security functionality provided by the CSP platform (TSF_CSP).
- FDP_ITC.2/TSS: FDP_ITC.2.1/TSS requires that the TSF shall enforce the Log message SFP when importing protocolData with Signature and audit records, controlled under the SFP, from CSP. FDP_ITC.2.2/TSS requires that the TSF shall use the security attributes associated with the imported user data. FDP_ITC.2.3/TSS requires that the TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the protocolData with Signature and audit records received. FDP_ITC.2.4/TSS requires that the TSF shall ensure that interpretation of the security attributes of the imported protocolData with Signature and audit records is as in-

tended by the source of the user data. FDP_ITC.2.5/TSS requires that the TSF shall enforce the following rules when importing protocolData with Signature and audit records controlled under the SFP from CSP: None. This is realized by TSF_Management, TSF_Log, TSF_Auth based on security functionality provided by the CSP platform (TSF_CSP).

- FDP_ITC.2/TD: FDP_ITC.2.1/TD requires that the TSF shall enforce the Log message SFP when importing Transaction Data controlled under the SFP, from outside of the TOE. FDP_ITC.2.2/TD requires that the TSF shall use the security attributes associated with the imported Transaction Data. FDP_ITC.2.3/TD requires that the TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the Transaction Data received. FDP_ITC.2.4/TD requires that the TSF shall ensure that interpretation of the security attributes of the imported Transaction Data is as intended by the source of the user data. FDP_ITC.2.5/TD requires that the TSF shall enforce the following rules when importing user data Transaction Data controlled under the SFP from outside of the TOE: (1) The TSF shall import the Transaction Data with the security attribute Serial Number of the ERS if the Serial Number of the ERS is in the set of accepted values according to FMT_MSA.1. If the Serial Number of the ERS is not in the set of accepted values the TSF must not import the Transaction Data. (2) The TSF shall import the Transaction Data with the security attribute Type of the Operation. (3) The Transaction Data shall be imported with the security attribute Transaction Number if the Type of the Operation is UpdateTransaction or FinishTransaction and the Transaction Number meets a Transaction Number of an ongoing transaction. (4) The TSF shall import Audit records from CSP. This is realized by TSF_Management, TSF_Log, TSF_Auth based on security functionality provided by the CSP platform (TSF_CSP).
- FDP_ITC.2/UCP_UD requires that the TSF shall enforce the update SFP when importing user data, controlled under the SFP, from the storage of the platform; that the TSF shall use the security attributes associated with the imported user data; that the TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the user data received; that the TSF shall ensure that interpretation of the security attributes of the imported user data is as intended by the source of the user data; and it requires that the TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: None. This is realized by TSF_Update and TSF_Log based on security functionality provided by the CSP platform (TSF_CSP).
- FDP_ETC.2/UCP_UD requires that the TSF shall enforce the update SFP when exporting user data, controlled under the SFP(s), outside of the TOE to the storage of the platform, that the TSF shall export the user data with the user data's associated security attributes, that the TSF shall ensure that the security attributes, when exported outside the TOE, are unambiguously associated with the exported user data, and that the TSF shall enforce rules when user data is exported from the TOE. This is realized by TSF_Update and TSF_Log based on security functionality provided by the CSP platform (TSF_CSP).
- FDP_RIP.1/UCP requires that the TSF shall ensure that any previous information content of a resource is made unavailable upon the deallocation of the resource after unsuccessful verification of the digital signature of the issuer by means of CSP the following objects: received Update Code Package. This is realized by TSF_Update and TSF_Log based on security functionality provided by the CSP platform (TSF_CSP).
- FIA_AFL.1 requires that the TSF shall detect when an administrator configurable positive integer within 1 – 15 unsuccessful authentication attempts occur related to PIN-based authentication, and that when the defined number of unsuccessful authentication attempts has been met, the TSF shall

delay the next authentication attempt or block the authentication, configurable by the administrator. This is realized by TSF_Management, TSF_Log and TSF_Auth based on security functionality provided by the CSP platform (TSF_CSP).

- FIA_ATD.1 requires the TSF shall maintain the following list of security attributes belonging to Administrator: (1) Identity, (2) Authentication Reference Data, (3) Role and (a) security attribute Identity, none belonging to the ERS (b) security attribute Identity, none belonging to the CSP. This is realized by TSF_Management, TSF_Log and TSF_Auth based on TSF_CSP.
- FIA_UAU.1: FIA_UAU.1.1 requires that the TSF shall allow (1) self test according to FPT_TST.1, (2) testing of external entity ERS according to FPT_TEE.1 and start the subject CTSS if testing was successful and the role CTSS interface is activated, (3) testing of external entity CSP according to FPT_TEE.1 and start the subject CSP if testing was successful, (4) none, on behalf of the user to be performed before the user is authenticated. FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user. This is realized by TSF_Management, TSF_Log and TSF_Auth based on TSF_CSP.
- FIA_UAU.5 requires that the TSF requires that the TSF shall provide password authentication to support user authentication, and that the TSF shall authenticate any user's claimed identity according to the rule that (1) password authentication shall be used for Administrator, (2) none. This is realized by TSF_Management, TSF_Log and TSF_Auth based on security functionality provided by the CSP platform (TSF_CSP).
- FIA_UAU.6 requires that the TSF shall re-authenticate the user under the conditions power on or reset. This is realized by TSF_Management and TSF_Auth based on security functionality provided by the CSP platform (TSF_CSP).
- FIA_UID.1 requires that the TSF shall allow self test according to FPT_TST.1 on behalf of the user to be performed before the user is identified, and that the TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user. This is realized by TSF_Management, TSF_Log and TSF_Auth based on TSF_CSP.
- FIA_USB.1.1: FIA_USB.1.1 requires that the TSF shall associate the following user security attributes with subjects acting on the behalf of that user (1) Identity, (2) Role. FIA_USB.1.2 requires that the TSF shall enforce the following rules on the initial association of user security attributeswith subjects acting on the behalf of users: the initial role of the user is Unidentified user. FIA_USB.1.3 requires that the TSF shall enforce the following rules governing changes to the user security attributesassociated with subjects acting on the behalf of users: (1) A subject is associated with attribute Identity and CTSS interface role after the ERS is successfully tested according to FPT_TEE.1. (2) A subject is associated with attribute Identity and CSP role after the CSP is successfully tested according to FPT_TEE.1. (3) A subject is associated with attribute Identity and Administrator role after successful authentication. (4) The Administrator is allowed to activate and deactivate the CTSS interface role. This is realized by TSF_Management, TSF_Log, TSF_Auth based on security functionality provided by the CSP platform (TSF_CSP).
- FMT_MOF.1 requires that the TSF shall restrict the ability to (1) enable and disable the functions password authentication according to FIA_UAU.5.2, clause (2) if defined to Administrator, (2) determine the behaviour of and modify the behaviour of the function FDP_ACF.1/LM by definition of a life time limit of ongoing transactions after which the transaction is terminated by the TSF to Administrator, (3) determine the behaviour of the function FPT_TEE.1 by definition of the identity and features to be tested of ERS to Administrator, (4) determine the behaviour of the function

FPT_TEE.1 by definition of the identity and features to be tested of CSP to Administrator, (5) determine the behaviour of and modify the behaviour of the function FPT_TEE.1 in case the test of CTSS interface component or CSP fails to Administrator. This is realized by TSF_Management, TSF_Log, TSF_Auth based on security functionality provided by the CSP platform (TSF_CSP).

- FMT_MSA.1 requires that the TSF shall enforce the Log message SFP and Update SFP to restrict the ability to (1) define the set of accepted values of the security attribute “Serial number of ERS” to Administrator, (2) define depending on the Serial number of ERS the identity of the signature-creation key to be used for the Transaction log to Administrator, (3) define depending on the Serial number of ERS the Serial number in the protocol data of Transaction log to Administrator, (4) define the identity of the signature-creation key to be used for the System logs and the Serial number in the protocol data of System logs to Administrator, (5) increase by 1 the internally stored security attribute “Transaction Number” when transaction is started to subjects in CTSS interface role, (6) modify the TD security attribute “Transaction Number” imported from the TD to none, (7) modify the security attributes of UCP to none. This is realized by TSF_Management, TSF_Log, TSF_Auth based on security functionality provided by the CSP platform (TSF_CSP).
- FMT_MSA.2 requires that the TSF shall ensure that only secure values are accepted for security attributes (1) Transaction Numbers building a strong increasing sequence without gaps, (2) Time stamps of the Log messages building a not decreasing sequence with consideration of adjustments of the CSP time source. This is realized by TSF_management, TSF_Log and TSF_Auth based on security functionality provided by the CSP platform (TSF_CSP).
- FMT_MSA.3 requires that the TSF shall enforce the Log message SFP and Update SFP to provide restrictive default values for security attributes that are used to enforce the SFP and that the TSF shall allow the none to specify alternative initial values to override the default values when an object or information is created. This is realized by TSF_Management.
- FMT_MSA.4 requires that the TSF shall use the following rules to set the value of security attributes: (1) The TSF uses the security attribute Serial Number of the ERS imported with Transaction Data to determine the signature-creation key be used by FDP_DAU.2/TS with ECDSA in [PPC-CSP-TS-Au] to sign the corresponding Log message as defined according to FMT_MSA.1. (2) If the Type of the Operation of imported Transaction Data is StartTransaction then the last internally generated Transaction Number shall be increased by 1 and this value shall be assigned to the ongoing transaction and the Transaction log of imported Transaction Data. (3) If the Type of the Operation of imported Transaction Data is UpdateTransaction or FinishTransaction and meets the Transaction Number of an ongoing transaction then the Transaction Number of the imported Transaction Data shall be assigned to the protocol data of the Transaction log. This is realized by TSF_Log, TSF_Auth based on security functionality provided by the CSP platform (TSF_CSP).
- FMT_MTD.1/AD requires that the TSF shall restrict the ability to (1) delete and create the Authentication Data Record of all authorized users to Administrator (2) modify the Authentication Reference Data to the corresponding authorized user. This is realized by TSF_Management and TSF_Auth based on security functionality provided by the CSP platform (TSF_CSP).
- FMT_MTD.1/SYSCTSS requires that the TSF shall restrict the ability to manual export and to clear after manual export the system logs to CTSS Interface Component. This is realized by TSF_Öog and TSF_Auth based on security functionality provided by the CSP platform (TSF_CSP).
- FMT_MTD.1/SYSAdmin requires that the TSF shall restrict the ability to select audited events in FAU_GEN.1/SYS, to define the number of audit records causing automatic export and clearing of exported audit records according to FAU_STG.3.1/SYS clause (1), and to define the percentage of

storage capacity of audit records if actions are assigned in FAU_STG.3.1/SYS clause (2) to the Administrator. This is realized by TSF_management, TSF_Log and TSF_Auth based on security functionality provided by the CSP platform (TSF_CSP).

- FMT_MTD.3/PW requires that the TSF shall ensure that only secure values are accepted for passwords and enforce changing initial passwords after first successful authentication of the user to a different secure operational password. This is realized by TSF_Management, TSF_Log and TSF_Auth based on security functionality provided by the CSP platform (TSF_CSP).
- FMT_SMF.1 requires that the TSF shall be capable of performing the following management functions: (1) management of security functions behavior, (2) management of Authentication Reference Data, (3) management of security attributes, (4) none. This is realized by TSF_Management, TSF_Log, TSF_Auth based on security functionality provided by the CSP platform (TSF_CSP).
- FMT_SMR.1 claims that the TSF shall shall maintain the roles Unidentified User, Administrator, Time Administrator, CTSS interface role and CSP role. This is realized by TSF_Management, TSF_Log, TSF_Auth based on security functionality provided by the CSP platform (TSF_CSP).
- FPT_TDC.1: FPT_TDC.1.1 requires that the TSF shall provide the capability to consistently interpret (1) Serial Number of the ERS, (2) Type of the Operation, (3) Transaction Number, (4) Signature Counter, (5) Time stamp, (6) Serial Number as hash value of the public key, (7) Signature when shared between the TSF and another trusted IT product. FPT_TDC.1.2 requires that the TSF shall use BSI TR-03151 [TR SE] and BSI TR-03153 [TR TSEA] when interpreting the TSF data from another trusted IT product. This is realized by TSF_Management, TSF_Log and TSF_Auth based on security functionality provided by the CSP platform (TSF_CSP).
- FPT_FLS.1 requires that the TSF shall preserve a secure state when the following types of failures occur: (1) self test according to FPT_TST.1 fails, (2) test of ESR according to FPT_TEE.1 fails, (3) test of CSP according to FPT_TEE.1 fails. The TSF shall exit the secure state only if the self-test, the test of the ESR and the test of the CSP are passed. This is realized by TSF_Auth based on security functionality provided by the CSP platform (TSF_CSP).
- FPT_TEE.1: FPT_TEE.1.1 requires that the TSF shall run a suite of tests during start-up, periodically during normal operation, user initiated shutdown and before exiting the secure state according to FPT_FLS.1 to check the fulfillment of (1) ESR Identity, none and (2) CSP Identity, none. The tests include the identification of the TOE to the tested device. FPT_TEE.1.2 requires that the TSF shall enter the secure state according to FPT_FLS.1 none additional action if the test fails. This is realized by TSF_Management based on security functionality provided by the CSP platform (TSF_CSP).
- FPT_TST.1: FPT_TST.1.1 requires that the TSF shall run a suite of self tests during initial start-up, at the request of the authorised user, periodically during normal operation and before exiting the secure state according to FPT_FLS.1 to demonstrate the correct operation of parts of TSF. FPT_TST.1.2 requires that the TSF shall provide authorised users with the capability to verify the integrity of TSF data. FPT_TST.1.3 requires that the TSF shall provide authorised users with the capability to verify the integrity of TSF implementation. This is realized by TSF_Management based on security functionality provided by the CSP platform (TSF_CSP).

9 References

In the following tables, the references used in this document are summarized.

Common Criteria

[CC_1]	Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; Version 3.1, Revision 5, April 2017; CCMB-2017-04-001.
[CC_2]	Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements; Version 3.1, Revision 5, April 2017; CCMB-2017-04-002.
[CC_3]	Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; Version 3.1, Revision 5, April 2017; CCMB-2017-04-003.
[CC_4]	Common Methodology for Information Technology Security Evaluation, Evaluation Methodology; Version 3.1, Revision 5, April 2017; CCMB-2017-04-004.

Protection Profiles

[PP CSP]	Common Criteria Protection Profile Cryptographic Service Provider, BSI-CC-PP-0104-2019
[PP CSPLight]	Common Criteria Protection Profile Cryptographic Service Provider Light, BSI-CC-PP-0111-2019
[PPC-CSP-TS-Au]	Common Criteria Protection Profile Configuration Cryptographic Service Provider – Time Stamp Service and Audit, BSI-CC-PP-0107-2019
[PPC-CSP-TS-Au-Cl]	Common Criteria Protection Profile Configuration Cryptographic Service Provider – Time Stamp Service and Audit - Clustering, BSI-CC-PP-0108-2019
[PPC-CSPLight-TS-Au-Cl]	Common Criteria Protection Profile Configuration Cryptographic Service Provider Light – Time Stamp Service and Audit - Clustering, BSI-CC-PP-0113-2019
[PP0105]	Common Criteria Protection Profile – Security Module Application for Electronic Record-keeping Systems, BSI-CC-PP-0105-V2-2020, Version 1.0.
[PP_Javacard]	Java Card Protection Profile - Open Configuration, Version 3.0 (May 2012), Published by Oracle, Inc.

TOE and Platform References

[ST_CSP]	cryptovision CSP – Java Card applet providing Cryptographic Service Provider, Security Target, BSI-DSZ-CC-1119.
[ST_Javacard]	Security Target Lite NXP JCOP 4.7 SE051, Rev. 2.1, 29 June 2022; Evaluation document, Public, NSCIB-CC-0095534-2MA.
[Zert_Javacard]	Certification Report NXP JCOP 4.7 SE051, Report number: NSCIB-CC-0095534-CR2, TÜV Rheinland Nederland B.V., 25 November 2021.

	with Assurance Continuity Maintenance Report JCOP 4.7 SE051, Report number: NSCIB-CC-0095534-2MA, TÜV Rheinland Nederland B.V., 05 July 2022.
[ST_IC]	NXP Secure Smart Card Controller N7121 with IC Dedicated Software and Crypto Library (R1/R2) - Security Target Lite - Rev. 2.5 — 4 May 2022, BSI-DSZ-CC-1136-V2.
[Zert_IC]	Certification Report BSI-DSZ-CC-1136-V2-2022 for NXP Secure Smart Card Controller N7121 with IC Dedicated Software and Crypto Library (R1/R2) from NXP Semiconductors Germany GmbH; 2022-06-02.
[Guidance]	cryptovision SMAERS – Java Card applet providing Security Module Application for Electronic Record-keeping Systems - Preparation Guidance (AGD_PRE).
[Guidance_OPE]	cryptovision SMAERS – Java Card applet providing Security Module Application for Electronic Record-keeping Systems - Operational Guidance (AGD_OPE).
[GP_CIC]	GlobalPlatform Card Common Implementation Configuration Version 1.0, February 2014
[AGD_PRE]	JCOP 4.7 SE051 - User manual for JCOP 4.7 SE051 (User Guidance and Administrator Manual), Rev. 1.3, 2021-09-27, NXP doc. no. 581813.
[TR03145]	BSI TR-03145-1, Secure CA operation, Part 1 - Generic requirements for Trust Centers instantiating as Certification Authority (CA) in a Public-Key Infrastructure (PKI) with security level 'high', Version 1.1, 27.03.2017
[AGD_PRE_CSP]	cryptovision CSP – Java Card applet providing Cryptographic Service Provider - Preparation Guidance (AGD_PRE).
[AGD_OPE_CSP]	cryptovision CSP – Java Card applet providing Cryptographic Service Provider - Operational Guidance (AGD_OPE).

References from the protection profile

[FCG]	Fiscal Code of Germany in the version promulgated on 1 October 2002 (Federal Law Gazette [Bundesgesetzblatt] I p. 3866; 2003 I p. 61), last amended by Article 6 of the Law of 18. July 2017 (Federal Law Gazette I p. 2745)
[KSV]	Verordnung zur Bestimmung der technischen Anforderungen an elektronische Aufzeichnungs- und Sicherungssysteme im Geschäftsverkehr (Kassensicherungsverordnung – KassenSichV), Bundesgesetzblatt Jahrgang 2017 Teil I Nr. 66, ausgegeben zu Bonn am 6. Oktober 2017
[TR ECC]	BSI, Elliptic Curve Cryptography, BSI Technical Guideline TR-03111, Version 2.10, 2018, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TR03111/BSI-TR-03111_V-2-1_pdf.pdf?__blob=publicationFile&v=2
[TR CryASE]	Technische Richtlinie BSI TR-03116 Kryptographische Vorgaben für Projekte der Bundesregierung Teil 5: Anwendungen der Secure Element API, 27. Januar 2020
[TR SE]	Technical Guideline BSI TR-03151 Secure Element API (SE API), Version 1.0.1, 20. Dezember 2018
[TR TSEA]	Technische Richtlinie BSI TR-03153 Technische Sicherheitseinrichtung für elektronische Aufzeichnungssysteme, Version 1.0.1, 20. Dezember 2018

[Klarstellungen]	Klarstellungen und Anwendungshinweise zu BSI TR03153 und BSI-CC-PP-0105-V2-2020, 13. November 2020, BSI
[AIS20]	BSI AIS 20/31, A proposal for: Functionality classes for random number generators, Version 2.0, 2011
[RFC5639]	M. Lochter, J. Merkle. Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation (RFC5639), 2010. Available at http://www.ietf.org/rfc/rfc5639.txt.
[ICAO]	ICAO, Machine Readable Travel Documents, ICAO Doc9303, Part 11: Security Mechanisms for MRTDSs, seventh edition, 2015
[NIST2005]	NIST Special Publication 800-38B Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication May 2005
[NIST2007]	NIST Special Publication 800-38D Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, November, 2007
[NIST2008]	FIPS PUB 198-1 The Keyed-Hash Message Authentication Code (HMAC), July 2008
[NIST 2013]	National Institute of Standards and Technology. FIPS PUB 186-4: Digital Signature Standard (DSS). 2013
[ISO/IEC 18033-3]	ISO/IEC 18033-3 Information technology - Security techniques, Encryption algorithms - Part 3: Block ciphers, 2010
[FIPS197]	Federal Information Processing Standards Publication 197 (FIPS PUB 197), Advanced Encryption Standard (AES), 2001

Keywords and Abbreviations

Term	Description
authentication verification data	data used by the user to authenticate themselves to the TOE
authenticity	the property that ensures that the identity of a subject or resource is the one claimed (cf. ISO/IEC 7498-2:1989)
cryptographic service provider	Component in the operational environment of the TOE providing cryptographic service for the TOE as defined in [PP CSP] with PP-module [PPC-CSP-TS-Au]
tax authorities	authority inspecting accounts and records in form of Log messages
certified technical security system (“zertifizierte technische Sicherheitseinrichtung”)	device dedicated to protect the electronic record-keeping system and digital records (cf. [FCG] section 146a sentence 2). It consists of a security module and a storage medium and providing the unified digital interface (cf. [FCG] section 146a sentence 3)
unified digital interface (“einheitliche digitale Schnittstelle”)	Interface for transmission or output of records or accounts for cash inspection according to [FCG] section 146b paragraph 2 sentence 2.
electronic record-keeping system	System that records each such business transaction or other procedure separately, completely (cf. FCG] section 146a paragraph 1)
taxpayer	taxpayer who is using an electronic record-keeping system for accounts and records (cf. [FCG] section 146a)

Table 6: Terminology

Acronym	Term
A.xxx	Assumption
CC	Common Criteria
CSP	cryptographic service provider, the TOE of [PP CSP] with PP-module [PPC-CSP-TS-Au]
CTSS	certified security device according to [FCG] section 146a sentence 2 (“zertifizierte technische Sicherheitseinrichtung”)
ERS	electronic record-keeping system according to [FCG] section 146a (1) sentence 1 (“elektronisches Aufzeichnungssystem”)
n. a.	not applicable
O.xxx	Security objective for the TOE
OE.xxx	Security objective for the TOE environment
OSP.xxx	Organisational security policy
SAR	Security assurance requirements

Acronym	Term
SFR	Security functional requirement
T.xxx	Threat
TD	Transaction data
TDS	Transaction data set
TDSS	Transaction data set sequence
TOE	Target of Evaluation
TSF	TOE security functions
UCP	Update Code Package

Table 7: Abbreviations